

VORLESUNGEN  
aus dem  
FACHBEREICH MATHEMATIK  
der  
UNIVERSITÄT ESSEN

Heft 30

Konkrete Charaktertafeln und kompatible Charaktere

Mathias Kratzer

Oktober 2001



## **Dissertation**

Zur Erlangung des Grades eines  
Doktors der Naturwissenschaften (Dr. rer. nat.)  
dem Fachbereich 6 (Mathematik und Informatik)  
der Universität Essen  
vorgelegt von  
Mathias Kratzer aus Planegg

Tag der Disputation: 22. Oktober 2001

Prüfungsausschussvorsitzender: Prof. Dr. Rüdiger Göbel  
1. Gutachter: Prof. Dr. Gerhard O. Michler  
2. Gutachter: Priv.-Doz. Dr. Wolfgang Lempken



# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Kurz gefasst . . . . .	1
1.2	Notation und Terminologie . . . . .	2
1.3	Danksagungen . . . . .	3
<b>2</b>	<b>Der Michler-Algorithmus</b>	<b>5</b>
2.1	Berechenbarkeit eines Einbettungsproblems . . . . .	5
2.2	Schritt für Schritt . . . . .	7
2.3	Uniforme Existenzbeweise für 25 sporadische Gruppen . . . . .	13
<b>3</b>	<b>Konkrete Charaktertafeln</b>	<b>15</b>
3.1	Präzisierung der fundamentalen Begriffe . . . . .	15
3.2	Der intuitive Lösungsansatz: ein Backtracking-Verfahren . . . . .	18
3.3	Konjugiertheitskriterien . . . . .	20
3.4	Beschleunigte Breitensuche . . . . .	24
3.5	Implementierung und qualitatives Laufzeitverhalten . . . . .	30
3.6	Berechnung der irreduziblen $\mathbb{C}$ -Charaktere . . . . .	34
<b>4</b>	<b>Kompatible Charaktere</b>	<b>41</b>
4.1	Der Vernetzungsgraph . . . . .	41
4.2	Algorithmische Konstruktion kompatibler Charaktere . . . . .	44
4.3	Implementierung und qualitatives Laufzeitverhalten . . . . .	49
<b>5</b>	<b>Ein Existenzbeweis für die Rudvalis-Gruppe</b>	<b>53</b>
5.1	Von der 2-Sylowuntergruppe zum Zentralisator . . . . .	53
5.2	Start des Michler-Algorithmus . . . . .	66
5.3	Normalisatorerweiterung gesucht . . . . .	68
5.4	Kompatible Paare, Probleme und ein Ausweg . . . . .	76
5.5	Das Endergebnis: 593775 Punkte . . . . .	82
<b>A</b>	<b>Die Rudvalis-Gruppe als Untergruppe von <math>SL_{133}(5)</math></b>	<b>87</b>
<b>B</b>	<b>Relationen aus dem Doppelnebenklassentrick</b>	<b>93</b>
<b>C</b>	<b>Eine konkrete Charaktertafel der Rudvalis-Gruppe</b>	<b>101</b>



# Kapitel 1

## Einleitung

### 1.1 Kurz gefasst

Mit voraus gerichtetem Blick auf ihr Hauptergebnis, einen neuen Existenzbeweis für die Rudvalis-Gruppe, lässt sich die vorliegende Arbeit als Beitrag zur Revision der Literatur über die sporadischen einfachen Gruppen verstehen. Tatsächlich würde eine derartige Einordnung mehr als die Hälfte des Inhalts thematisch unterschlagen; genau diesem Effekt entgegenwirken soll der alles andere als direkt auf das Klassifikationsprojekt der einfachen endlichen Gruppen hinweisende Titel „Konkrete Charaktertafeln und kompatible Charaktere“.

Unbestreitbar birgt der in Kapitel 2 beschriebene Algorithmus von G. O. Michler prinzipiell die Möglichkeit der uniformen Konstruktion aller 26 bekannten und laut Klassifikationssatz einzigen sporadischen einfachen Gruppen. So bemerkenswert dieser Umstand auch sein mag, muss er als eine Art naturgegebenes Phänomen betrachtet werden, denn das erklärte Ziel des Michlerschen Verfahrens ist die Lösung eines relativ speziellen und deshalb per Computer (nicht bloß im Sinne der theoretischen Informatik) berechenbaren Einbettungsproblems.

Von zwei Gruppen  $G$  und  $H$  mit isomorphen Untergruppen  $U \leq G$  und  $V \leq H$  ist dabei an einem gewissen Punkt zu entscheiden, ob sie innerhalb einer gemeinsamen Obergruppe mit zu  $U \cong V$  isomorphem Schnitt auftreten können. Eine darstellungstheoretische Umformulierung dieser Frage führt schließlich auf den allgemeinen Begriff der *Kompatibilität zwischen Charakteren* zweier verschiedener Gruppen.

Wie sich herausstellt, reicht es für einen Test auf Kompatibilität nicht aus, Charaktere als von der ihnen zugrunde liegenden Gruppe losgelöste, abstrakte mathematische Objekte aufzufassen. Wesentliche Faktoren sind vielmehr die konsistente Identifikation der irreduziblen Charaktere von  $U$  mit denen von  $V$  sowie die Fusion der Konjugiertenklassen von  $U$  in  $G$  bzw. von  $V$  in  $H$ . Definitive Aussagen über Kompatibilität sind daher nur zu gewinnen, wenn die betreffenden Charaktere als Funktionen auf konkreten Gruppen leben und nicht zu einem Tupel von Körperelementen reduziert werden.

Kapitel 3 behandelt Konzepte und Methoden, um eine einmal bestimmte *konkrete Charaktertafel* durch die Bindung an ein lexikographisch standardisiertes Repräsentantensystem für die Konjugiertenklassen der jeweiligen Gruppe  $G$  problemlos auf isomorphe Kopien von  $G$  übertragen zu können und die funktionelle Verbindung zwischen Tafel und Gruppe unabhängig von der verwendeten Computeralgebra-Software dauerhaft zu fixieren.

Die mit Abstand effizienteste Strategie bei der *Suche nach allen Paaren* kompatibler Charaktere, deren Grad eine gegebene Schranke nicht übersteigt, ist ohne Zweifel ihre planmäßige Konstruktion aus irreduziblen Bestandteilen. Da sich dieses Vorhaben jedoch als echte kombinatorische Herausforderung erweist, wird in Kapitel 4 zunächst ein graphentheoretisches Modell des Kompatibilitätsbegriffs kreiert, welches die ursprünglich rein verbale Aufgabenstellung einer formalen Spezifikation zugänglich macht und obendrein auch noch den adäquaten Lösungsweg aufzeigt: einen Backtracking-Algorithmus.

Sämtliche der in Kapitel 3 und 4 entwickelten Verfahren wurden vom Autor in den systemeigenen Sprachen gängiger Computeralgebrapakete — GAP [39], [13] oder/und MAGMA [2] — implementiert und getestet. Ein komplexes Anwendungsbeispiel dokumentiert schließlich Kapitel 5 mit dem schon erwähnten Existenzbeweis für die Rudvalis-Gruppe.

## 1.2 Notation und Terminologie

Um semantischen Missverständnissen vorzubeugen, werden nun einige Bezeichnungen und Definitionen aus dem Bereich der Gruppentheorie festgelegt.

Sei  $G$  eine endliche Gruppe. Die Elemente von  $G$  verknüpfen wir im Folgenden multiplikativ, sprich ohne ausdrückliches Operatorsymbol. Unter der **Konjugation mit**  $g \in G$  verstehen wir den von  $g$  induzierten inneren Automorphismus

$$\kappa_g : G \rightarrow G, \quad x \mapsto x^g := g^{-1}xg \quad (\text{nicht etwa } gxg^{-1}!).$$

Zwei Elemente  $x, y \in G$  heißen **zueinander konjugiert in**  $G$ , in Zeichen

$$x \sim_G y,$$

wenn ein  $g \in G$  mit  $\kappa_g(x) = x^g = y$  existiert.

Per Konjugation operiert eine jede Gruppe auf sich selbst. Für ein Element  $x \in G$  ist der  $G$ -Orbit  $(x)^G$  unter ebendieser Operation die Menge aller in  $G$  zu  $x$  konjugierten Elemente und heißt die **Konjugiertenklasse von**  $x$  in  $G$ .

In Übereinstimmung mit GAP und MAGMA evaluiert der **Kommutator**  $[x, y]$  definitionsgemäß stets zum selben Wert wie der Ausdruck

$$x^{-1}y^{-1}xy \quad (\text{nicht etwa } xyx^{-1}y^{-1}!).$$

Etwas ausführlicher denn gewohnt schreiben wir ferner das kanonische **innere Produkt** zweier Klassenfunktionen  $\varphi, \psi : G \rightarrow \mathbb{C}$  als

$$[\varphi, \psi]_G.$$

Sonstige nicht explizit definierte Schreib- oder Redeweisen aus dem Bereich der Theorie der endlichen Gruppen findet der Leser im gleichnamigen Lehrbuch von H. Kurzweil und B. Stellmacher [24] erklärt. Eine ganz entsprechende Primärreferenz zu Symbolik und Vokabular der Charaktertheorie steht mit dem Standardwerk von I. M. Isaacs [18] zur Verfügung.

Für das Nachschlagen inhaltlicher Zusammenhänge eignen sich neben den bereits genannten natürlich auch die Kompendien von B. Huppert [17] bzw. C. W. Curtis und I. Reiner [11].



## 1.3 Danksagungen

Diese Seite widme ich all jenen, die einen nicht unerheblichen Teil ihrer Zeit dem Zustandekommen der restlichen 111 Seiten geopfert haben.

Mein erster und besonderer Dank gilt meinem Doktorvater *Prof. Dr. Gerhard O. Michler*: Für sein sowohl in fachlicher wie in persönlicher Hinsicht absolut außerordentliches Engagement, für die von Beginn an unschätzbar vertrauensvolle und enge Zusammenarbeit mit ihm und vor allem für sein auch gegenüber sehr offenen Worten stets mindestens ebenso offenes Ohr. — Es war mir eine ausgesprochene Ehre, der „30-ste“ sein zu dürfen!

Bedanken möchte ich mich des Weiteren bei *PD Dr. Wolfgang Lempken*. Ohne sein scheinbar grenzenloses Wissen um die Interna gewisser Matrixgruppen wäre Kapitel 5 wahrscheinlich rechtzeitig zur nächsten Jahrhundertwende fertig geworden.

— Danke für die „Nachhilfestunden“!

Ungezählte hilfreiche Tipps, dringend notwendige Ideen sowie konstruktive Verbesserungsvorschläge verdanke ich den informativen Fachsimpeleien mit meinen beiden Zimmerkollegen respektive (inzwischen leider -ex)-nachbarn am Institut für Experimentelle Mathematik, den *Dres. Michael Weller* und *Volker Gebhardt*.

— Euer algorithmisches Know-how ist unschlagbar!

Gewiss: Über Geld spricht man nicht. Doch schließlich *schreibe* ich ja und Dank gebührt dafür in jedem Fall der *Deutschen Forschungsgemeinschaft (DFG)*, die mich im Rahmen des Graduiertenkollegs „Theoretische und experimentelle Methoden der Reinen Mathematik“ über die letzten knapp drei Jahre hinweg mit einem Promotionsstipendium unterstützt hat.

Meinen Eltern *Hermine* und *Wolfgang* danke ich für das unermüdliche Korrekturlesen des Manuskripts nach den Regeln der neuen deutschen Rechtschreibung.

— Der ganze Duden ist wertlos ohne das Adlerauge eines Lehrers!

Zwei Menschen schulde ich letztendlich ganze Wagenladungen voller Dankeschöns; einer davon ist *Prof. Dr. Kurt Meyberg* von der Technischen Universität München, der 1998 auf die Frage nach einem „guten Studenten“ sofort an einen seiner Diplomanden gedacht hat.

— Ihr Ratschlag war (wie immer) Gold wert!

Dennoch hätten mich zwei Professoren damals weder alleine noch zusammen mit den sprichwörtlichen zehn Pferden von München ins Ruhrgebiet gebracht. Dazu bedurfte es schon der Courage, der Energie und der Unternehmungslust meiner Ehefrau *Bettina*, der ich hiermit auch die übrigen 111 Seiten widme.

— Dein „Mach’s, ich geh’ mit ...“ gab den Ausschlag!



## Kapitel 2

# Der Michler-Algorithmus

Nahezu alle im Rahmen dieser Arbeit behandelten Probleme und Fragestellungen sind motiviert durch einen von G. O. Michler entwickelten und in [30] ausführlich beschriebenen Algorithmus zur Konstruktion gewisser endlicher einfacher Gruppen. Eine grobe Skizzierung dieses Verfahrens erscheint also nicht nur sinnvoll, weil wir es in Kapitel 5 schließlich explizit anwenden wollen, sondern bietet dem Leser außerdem die Gelegenheit, sich mit dem fundamentalen Vokabular der folgenden Kapitel vertraut zu machen.

### 2.1 Berechenbarkeit eines Einbettungsproblems

Gegeben sei eine beliebige endliche Gruppe  $H$ . Gesucht werden bis auf Isomorphie alle *einfachen* endlichen Gruppen  $G$ , in welche sich  $H$  als Untergruppe einbetten lässt oder, anders ausgedrückt, die eine zu  $H$  isomorphe Untergruppe besitzen.

Kann ein Rechenautomat existieren, der diese Aufgabe in endlicher Zeit löst? So lautet die Frage nach der Berechenbarkeit des oben beschriebenen klassischen Einbettungsproblems der Gruppentheorie, und die Antwort liegt auf der Hand: Nein! Denn bereits im Fall einer zyklischen Gruppe  $H$  wären unter anderem fast alle alternierenden Gruppen  $A_n$ ,  $n \geq 5$ , das heißt unendlich viele Objekte zu konstruieren.

Tatsächlich zeigt ein berühmtes Resultat von R. Brauer und K. A. Fowler, dass Unberechenbarkeit hier lediglich die Folge einer zu allgemeinen Problemformulierung ist:

**Satz 2.1.1** (BRAUER-FOWLER)

*Es sei  $G$  eine einfache endliche Gruppe,  $t$  eine Involution in  $G$  und  $n := |\mathbf{C}_G(t)|$ . Dann gilt:*

$$|G| \leq (2n^2)! .$$

**Bemerkung:** Enthält  $G$  mindestens zwei Konjugiertenklassen von Involutionen, gilt sogar die ungleich schärfere Schranke  $|G| < n^3$ . Beide Abschätzungen wurden in [3] natürlich unabhängig vom Klassifikationssatz für einfache endliche Gruppen bewiesen, der erst gut 30 Jahre später aufgestellt werden sollte.

Da es nur endlich viele Gruppen gibt, deren Ordnung kleiner als eine gegebene Schranke ist, existieren nach Satz 2.1.1 insbesondere nur endlich viele einfache Gruppen  $G$ , in denen eine

vorgegebene Gruppe  $H$  die Rolle eines Involutionenzentralisators spielt. Obschon ihrer absolut unkonstruktiven Natur stellt diese Aussage das entscheidende Argument für den Beweis der Berechenbarkeit des vergleichsweise speziellen Einbettungsproblems

Gegeben sei eine beliebige endliche Gruppe  $H$ . Gesucht werden bis auf Isomorphie alle einfachen endlichen Gruppen  $G$ , die eine Involution  $t$  mit  $\mathbf{C}_G(t) \cong H$  enthalten.

dar, denn die Gesamtheit der endlichen Gruppen ist eine aufzählbare Menge. Um den letzteren Sachverhalt einzusehen, denke man etwa an einen Algorithmus, der zu jeder natürlichen Zahl  $d$  der Reihe nach alle möglichen  $d \times d$ -Verknüpfungstafeln erzeugt und auf das Erfülltsein der Gruppenaxiome hin testet.

Ein solch naiver Algorithmus leistet freilich kaum mehr als theoretische Dienste. Wer ein praktisch nutzbares Verfahren bevorzugt, muss zweifellos etwas investieren, zum Beispiel ein paar Zusatzvoraussetzungen — über die Gruppe  $G$  oder/und über die Involution  $t$ .

**Definition 2.1.2** (2-Zentralität)

Sei  $G$  eine endliche Gruppe.

Ein Element von  $G$  heißt **2-zentral**, wenn es im Zentrum einer 2-Sylowuntergruppe von  $G$  enthalten ist.

**Definition 2.1.3** (Multiplizitätenfreiheit)

Sei  $G$  eine endliche Gruppe und  $\mathbb{F}$  ein Körper.

Ein  $G$ -Modul über  $\mathbb{F}$  [ eine  $\mathbb{F}$ -Darstellung von  $G$  / ein  $\mathbb{F}$ -Charakter von  $G$  ] heißt **multiplizitätenfrei**, wenn er [ sie / er ] sich aus paarweise nicht-isomorphen [ nicht-ähnlichen / verschiedenen ] irreduziblen Konstituenten zusammensetzt.

Mit Hilfe der soeben eingeführten Begriffe sind wir nun in der Lage, ein noch spezielleres Einbettungsproblem zu beschreiben:

Gegeben sei eine beliebige endliche Gruppe  $H$ . Gesucht werden bis auf Isomorphie alle einfachen endlichen Gruppen  $G$ , die eine 2-zentrale Involution  $z$  enthalten und den folgenden drei Bedingungen genügen:

1. Es gibt einen Isomorphismus  $\tau : \mathbf{C}_G(z) \rightarrow H$ ;
2. Eine (und damit jede) 2-Sylowuntergruppe  $S$  von  $H$  enthält einen elementar abelschen Normalteiler  $A \trianglelefteq S$  maximaler Ordnung  $|A| \geq 4$  derart, dass

$$G = \langle \mathbf{C}_G(z), N := \mathbf{N}_G(\tau^{-1}(A)) \rangle ;$$

3. Für eine Primzahl  $p < |H|^2 - 1$  mit  $\text{ggT}(p, |H||N|) = 1$  besitzt  $G$  eine irreduzible  $p$ -modulare Darstellung  $\mathfrak{X}$ , deren Restriktion auf  $\mathbf{C}_G(z)$  multiplizitätenfrei ist.

Selbstverständlich ist auch dieses Einbettungsproblem berechenbar. Für seine Lösung existiert mit dem Michler-Algorithmus allerdings ein weitaus effizienteres Verfahren als das sukzessive Generieren und Kontrollieren von Verknüpfungstafeln.

## 2.2 Schritt für Schritt

Das strukturelle und inhaltliche Gerüst dieses Abschnitts bildet der Algorithmus 4.6 aus [30]. Wo es mit Blick auf Kapitel 5 sinnvoll bzw. vertretbar erschien, wurden anwendungsrelevante Hinweise ergänzt bzw. rein implementierungstechnische Details weggelassen.

Unser Hauptaugenmerk soll hier vor allem denjenigen Teilschritten des Verfahrens gewidmet sein, welche genau genommen erst durch den Einsatz der in den Kapiteln 3 und 4 entwickelten Werkzeuge und Methoden realisierbar werden. Für einen Korrektheits- und Terminierungsbeweis sei der interessierte Leser daher auf die oben zitierte Originalarbeit verwiesen.

### 2.2.1 Pre-processing des Eingabeparameters

Anhand der folgenden Aussage wird unmittelbar klar, welch ein bedeutender Informationsträger der Zentralisator einer 2-zentralen Involution ist.

#### Lemma 2.2.1

*Es sei  $G$  eine endliche Gruppe und  $z \in G$  eine 2-zentrale Involution. Dann gilt:*

$$S \in \text{Syl}_2(\mathbf{C}_G(z)) \implies S \in \text{Syl}_2(G) .$$

**Beweis.** Gemäß Definition 2.1.2 existiert eine 2-Sylowuntergruppe  $T$  von  $G$  mit  $z \in \mathbf{Z}(T)$ , also  $T \leq \mathbf{C}_G(z)$ . Hieraus folgt  $T \in \text{Syl}_2(\mathbf{C}_G(z))$  und, da alle 2-Sylowuntergruppen paarweise konjugiert sind, auch schon die Behauptung.  $\square$

Entsprechend des zu lösenden Einbettungsproblems sei nun eine endliche Gruppe  $H$  gegeben. Fast ohne weitere Rechnung lassen sich a priori bereits zwei Fälle unterscheiden:

- Falls  $|\mathbf{Z}(H)|$  ungerade ist, kann eine zu  $H$  isomorphe Gruppe niemals der Zentralisator einer Involution sein. Deshalb brauchen wir den Michler-Algorithmus in dieser Situation erst gar nicht zu starten.
- Falls jedoch  $|\mathbf{Z}(H)|$  gerade ist, dürfen wir dank Lemma 2.2.1 ohne Beschränkung der Allgemeinheit *irgendeine* 2-Sylowuntergruppe  $S$  von  $H$  fixieren. Jede ebenso ein für alle Mal fest ausgewählte Involution  $z \in \mathbf{Z}(H)$  liegt dann garantiert auch in  $\mathbf{Z}(S)$ , so dass in den zu konstruierenden Gruppen  $G$  mit Isomorphismus  $\tau : \mathbf{C}_G(\cdot) \rightarrow H$  das jeweilige Urbild  $\tau^{-1}(z)$  den Part einer 2-zentralen Involution übernehmen kann.

Die auf diese Weise erklärten zusätzlichen Objekte  $S$  und  $z$  komplettieren intern den formal nur aus der Gruppe  $H$  bestehenden Satz von Eingabeparametern des Michler-Algorithmus.

### 2.2.2 Elementar abelsche Normalteiler maximaler Ordnung

#### **Schritt 1**

Bestimme die Menge  $\mathfrak{A}$  aller elementar abelschen Normalteiler  $A \trianglelefteq S$  von maximaler Ordnung  $|A| \geq 4$  in Bezug auf die folgenden zwei Eigenschaften:

- (a)  $D := D(A) := \mathbf{N}_H(A) < H$  ;
- (b)  $C := C(A) := \mathbf{C}_H(A) \implies \mathbf{Z}(C)$  ist eine 2-Gruppe .

**Für**  $A \in \mathfrak{A}$  : Führe jeden der noch folgenden Schritte aus ...

Man beachte, dass im Falle einer elementar abelschen 2-Sylowuntergruppe  $S$  die Wahl des trivialen Normalteilers  $A = S$  ausdrücklich erlaubt ist. Exakt aus diesem Grund ist hier nicht von „maximalen Normalteilern“, sondern von „Normalteilern maximaler Ordnung“ die Rede.

### 2.2.3 Zulässige Gruppenerweiterungen

#### **Schritt 2**

Fasse  $A$  als  $\text{GF}(2)$ -Vektorraum der Dimension  $d := \log_2 |A|$  auf und fixiere sodann eine geordnete Basis  $(a_1 = z, a_2, \dots, a_d)$  von  $A$ .

Berechne bezüglich dieser Basis den durch die Konjugationsoperation von  $D$  auf  $A$  induzierten Homomorphismus  $\eta : D \rightarrow \text{GL}_d(2)$  mit Kern  $C$  und Bild  $\Delta := \eta(D)$ .

Bestimme schließlich die Menge  $\mathfrak{S}(A)$  aller Untergruppen  $\Phi \leq \text{GL}_d(2)$  von maximaler Ordnung in Bezug auf die folgenden drei Eigenschaften:

- (a)  $\Delta = \text{Stab}_\Phi(z) < \Phi$ ;
- (b)  $|\Phi : \Delta|$  ist ungerade;
- (c) es existiert eine Gruppenerweiterung  $1 \rightarrow C \rightarrow E_\Phi \rightarrow \Phi \rightarrow 1$  zusammen mit einer Einbettung  $\mu : D \hookrightarrow E_\Phi$  derart, dass das Diagramm

$$\begin{array}{ccccccc}
 1 & \longrightarrow & C & \longrightarrow & E_\Phi & \longrightarrow & \Phi \longrightarrow 1 \\
 & & \uparrow \text{Id}_C & & \uparrow \mu & & \uparrow \text{Id}_\Phi \\
 1 & \longrightarrow & C & \xrightarrow{\text{Id}_D} & D & \xrightarrow{\eta} & \Delta \longrightarrow 1
 \end{array}$$

kommutiert.

**Für  $\Phi \in \mathfrak{S}(A)$  :** Führe jeden der noch folgenden Schritte aus ...

Um die Erweiterungsgruppen  $E_\Phi$  und zugehörige Einbettungen  $\mu$  zu konstruieren, bedarf es in der Praxis zunächst einer gründlichen Strukturanalyse des Normalisators  $D$ . Das angestrebte Ziel ist eine endliche Präsentation von  $D$ , die dann (eventuell auf verschiedene Arten und Weisen) zu einer endlichen Präsentation von  $E_\Phi$  fortgesetzt werden kann. Die dazu passende Einbettung  $\mu$  ergibt sich auf diesem Weg quasi von selbst.

Weil  $A$  normal in  $S$  ist, gilt natürlich immer  $S \leq D$ , und im Allgemeinen existieren zu einer Isomorphieklasse von möglichen Erweiterungsgruppen  $E_\Phi$  mehrere Einbettungen  $\mu$ , die das Diagramm in Bedingung (c) kommutieren lassen.

### 2.2.4 Paare kompatibler Charaktere

Im nun anstehenden dritten Schritt des Michler-Algorithmus sehen wir uns endlich mit den beiden zentralen Begriffen dieser Arbeit konfrontiert. Während einer von ihnen implizit ins Spiel kommen wird, tritt der andere direkt auf den Plan. Der bequemeren Formulierbarkeit halber erweitern wir allerdings vorab noch unser Symbolikrepertoire.

**Definition 2.2.2** (Ring der komplexwertigen Charaktere und spezielle Teilmengen)

Für eine endliche Gruppe  $G$  bezeichne

$\text{Char}_{\mathbb{C}}(G)$  den Ring der  $\mathbb{C}$ -Charaktere von  $G$ ,

$\underline{\text{Char}}_{\mathbb{C}}(G)$  die Teilmenge der treuen Elemente von  $\text{Char}_{\mathbb{C}}(G)$  und

$\underline{\text{Char}}_{\mathbb{C}}^{\sharp}(G)$  die Teilmenge der multiplizitätenfreien Elemente von  $\underline{\text{Char}}_{\mathbb{C}}(G)$ .

Vorausschauend auf Kapitel 4 ist die folgende Definition ein wenig allgemeiner gehalten als ihr Pendant 3.4 in [30].

**Definition 2.2.3** (Kompatibilität komplexwertiger Charaktere)

Seien  $K$  und  $L$  endliche Gruppen sowie  $U \leq K$  und  $V \leq L$  mit  $U \cong V$ .

Ein Charakter  $\varphi \in \text{Char}_{\mathbb{C}}(K)$  heißt **über  $U$  kompatibel zu** einem Charakter  $\psi \in \text{Char}_{\mathbb{C}}(L)$ , wenn  $\varphi \downarrow_U = \psi \downarrow_V$  gilt.

Gegebenenfalls heißt abkürzend auch das Paar  $(\varphi, \psi)$  **über  $U$  kompatibel** und wir nennen dann den gemeinsamen Grad

$$\deg(\varphi, \psi) := \varphi(1_K) = \psi(1_L)$$

den **Grad** dieses Paares.

Das Gleichheitszeichen zwischen zwei Charaktere zu setzen, die auf verschiedenen Gruppen leben, mag gewöhnungsbedürftig erscheinen. Nichtsdestoweniger ist es in der Situation von Definition 2.2.3 gerechtfertigt:

Weil die Untergruppen  $U$  und  $V$  isomorph sind, lassen sich ihre Charaktertafeln durch geeignete Zeilen- (bzw. Charakter-) und Spalten-(bzw. Konjugiertenklassen-)vertauschungen ineinander überführen. Diese Identifikation der Elemente von  $\text{Irr}_{\mathbb{C}}(U)$  mit denen von  $\text{Irr}_{\mathbb{C}}(V)$  ist dann aus Linearitätsgründen zu einer Äquivalenzrelation  $=$  auf das gesamte kartesische Produkt  $\text{Char}_{\mathbb{C}}(U) \times \text{Char}_{\mathbb{C}}(V)$  fortsetzbar.

Sofern ein expliziter Isomorphismus  $\alpha : U \rightarrow V$  bekannt ist und die Charaktertafel von  $V$  über dem  $\alpha$ -Bild eines fest gewählten Konjugiertenklassenrepräsentantensystems von  $U$  berechnet wurde, reichen sogar Zeilenvertauschungen alleine aus, um die Tafel von  $U$  mit der von  $V$  zur Deckung zu bringen.

Diese Überlegung macht deutlich, warum es beispielsweise für die algorithmische Suche nach kompatiblen Charakteren von erheblichem Nutzen ist, auf so genannten *konkreten* Charaktertafeln operieren zu können, deren Spalten mit konkreten Konjugiertenklassenrepräsentanten der zugrunde liegenden Gruppe „beschriftet“ sind.

Ein rechnerisch denkbar einfacher Fall liegt schließlich vor, wenn  $U$  und  $V$  — wie im Michler-Algorithmus  $D$  und  $\mu(D)!$  — von denselben abstrakten Erzeugern generiert werden und die Repräsentanten der Konjugiertenklassen von  $U$  als Worte in diesen Erzeugern verfügbar sind. Wie ein derartiges Repräsentantensystem bestimmt werden kann, soll Kapitel 3 klären.

**Schritt 3**

Berechne konkrete Charaktertafeln für die Gruppen  $H$ ,  $E_\Phi$ ,  $D$  und  $\mu(D)$ .  
 Berechne die Fusion der Konjugiertenklassen von  $D$  in die von  $H$ .  
 Berechne die Fusion der Konjugiertenklassen von  $\mu(D)$  in die von  $E_\Phi$ .  
 Bestimme die Menge  $\Pi$  aller über  $U$  kompatiblen Paare  $(\chi, \vartheta) \in \underline{\text{Char}}_{\mathbb{C}}^{\sharp}(H) \times \underline{\text{Char}}_{\mathbb{C}}(E_\Phi)$ .  
**Für**  $(\chi, \vartheta) \in \Pi$  : Führe jeden der noch folgenden Schritte aus ...

Laut Proposition 3.5 in [30] ist  $\Pi$  eine endliche Menge und demnach auf der Grundlage der zuvor ermittelten Charaktertafel- und Fusionsinformation theoretisch berechenbar. Bereits für Gruppen mit relativ wenig irreduziblen Charakteren lehrt uns jedoch spätestens die experimentelle Erfahrung, dass die Menge  $\underline{\text{Char}}_{\mathbb{C}}^{\sharp}(H) \times \underline{\text{Char}}_{\mathbb{C}}(E_\Phi)$  der als Elemente von  $\Pi$  in Frage kommenden Charakterpaare hoffnungslos zu groß gerät.

Praktische Anwendungen des Michler-Algorithmus begnügen sich daher fast ausnahmslos mit der Konstruktion aller kompatiblen Paare, deren Grad eine moderat höher als minimal gewählte Schranke nicht überschreitet.

**2.2.5 Amalgamierung**

Es gilt nun,  $H$  und  $E_\Phi$  in dieselbe generelle lineare Gruppe einzubetten — und zwar derart, dass sie sich dort genau im Bild von  $D$  bzw.  $\mu(D)$  schneiden. Während die Kompatibilität von  $\chi$  und  $\vartheta$  über  $D$  die Existenz einer solchen Einbettung garantiert, legt der Grad  $\deg(\chi, \vartheta)$  zudem den Rang des benötigten Matrix-Universums fest. Somit verbleibt nurmehr zu klären, auf wieviele *effektiv verschiedene* Arten und Weisen eine Einbettung realisiert werden kann. Der Beantwortung dieser Frage dient die Amalgam-Methode:

**Schritt 4**

Setze  $\ell := |H|^2 - 1$ .  
 Setze  $n := \deg(\chi, \vartheta)$ .  
 Bestimme die Menge  $P$  aller Primzahlen  $p < \ell$  mit  $\text{ggT}(|H||E_\Phi|, p) = 1$ .  
**Für**  $p \in P$  :  
   Bestimme den Zerfällungskörper  $\mathbb{F}$  der alternierenden Gruppe  $A_\ell$  mit  $\text{char}(\mathbb{F}) = p$ .  
   Führe jeden der noch folgenden Schritte aus ...

**Schritt 4a**

Konstruiere den zu  $\chi$  korrespondierenden, halbeinfachen  $\mathbb{F}H$ -Modul  $M$ .  
 Konstruiere den zu  $\vartheta$  korrespondierenden, halbeinfachen  $\mathbb{F}E_\Phi$ -Modul  $N$ .

Die irreduziblen direkten Summanden von  $M$  bzw.  $N$  gewinnt man wohl am schnellsten durch sukzessive Anwendung von R. A. Parkers MEAT-AXE [34] auf

1. einen treuen Permutationsmodul von  $H$  bzw.  $E_\Phi$  und
2. geeignete Tensorprodukte zwischen den irreduziblen Konstituenten dieses Moduls.

Beim Übersetzen zwischen irreduziblen  $\mathbb{C}$ -Charakteren und korrespondierenden  $\mathbb{F}$ -Moduln erweisen sich konkrete Charaktertafeln erneut als unerlässliches Hilfsmittel. Moduln gleicher Dimension (präziser: die von ihnen induzierten Darstellungen) können nämlich in der Regel nur anhand expliziter Spurberechnungen eindeutig gewissen Charakteren zugeordnet werden.



**Schritt 4b**

Berechne die von  $M$  induzierte  $\mathbb{F}$ -Darstellung  $\mathfrak{M}$  von  $H$ .

Berechne die von  $N$  induzierte  $\mathbb{F}$ -Darstellung  $\mathfrak{N}$  von  $E_\Phi$ .

Bestimme eine Transformationsmatrix  $T \in \mathrm{GL}_n(\mathbb{F})$  mit

$$T^{-1}\mathfrak{N}(\mu(x))T = \mathfrak{M}(x) \quad \text{für alle } x \in D.$$

*/\** Solch ein  $T$  existiert, denn  $\mathfrak{N} \circ \mu$  und  $\mathfrak{M}|_D$  sind ähnliche  $\mathbb{F}$ -Darstellungen von  $D$ . *\*/*

Identifiziere  $H$  mit  $\mathfrak{M}(H) \leq \mathrm{GL}_n(\mathbb{F})$  und  $E_\Phi$  mit  $\mathfrak{N}(E_\Phi)^T \leq \mathrm{GL}_n(\mathbb{F})$ .

Berechne eine Doppelnebenklassenzerlegung

$$\mathbf{C}_{\mathrm{GL}_n(\mathbb{F})}(D) = \bigcup_{i=1}^s \mathbf{C}_{\mathrm{GL}_n(\mathbb{F})}(H) \cdot R_i \cdot \mathbf{C}_{\mathrm{GL}_n(\mathbb{F})}(E_\Phi) .$$

Die paarweise verschiedenen  $\mathbf{C}_{\mathrm{GL}_n(\mathbb{F})}(H)$ - $\mathbf{C}_{\mathrm{GL}_n(\mathbb{F})}(E_\Phi)$ -Doppelnebenklassen in  $\mathbf{C}_{\mathrm{GL}_n(\mathbb{F})}(D)$  stehen nach J. G. Thompson [43] in einer 1:1-Beziehung zu den paarweise nicht-ähnlichen  $n$ -dimensionalen  $\mathbb{F}$ -Darstellungen des freien amalgamierten Produkts von  $H$  und  $E_\Phi$  über der gemeinsamen Untergruppe  $D$ . Ihre Anzahl  $s$  lässt sich unter gewissen Voraussetzungen sehr einfach berechnen.

**Definition 2.2.4** (Minimalität kompatibler Charakterpaare)

Seien  $K$  und  $L$  endliche Gruppen sowie  $U \leq K$  und  $V \leq L$  mit  $U \cong V$ .

Ein über  $U$  kompatibles Paar  $(\varphi, \psi) \in \mathrm{Char}_{\mathbb{C}}(K) \times \mathrm{Char}_{\mathbb{C}}(L)$  heißt **minimal**, wenn kein echter Konstituent  $\varphi_0$  von  $\varphi$  über  $U$  kompatibel zu einem Konstituenten von  $\psi$  ist.

**Bemerkung:** Kompatible Paare minimalen Grades sind trivialerweise auch minimal im Sinne von Definition 2.2.4. Die Umkehrung dieser Aussage ist aber im Allgemeinen falsch!

**Lemma 2.2.5**

In der Situation von **Schritt 4b** sei  $(\chi, \vartheta)$  ein minimales kompatibles Paar, und die gemeinsame Restriktion  $\delta$  von  $\chi$  und  $\vartheta$  auf  $D$  sei multiplizitätenfrei. Ferner bezeichne  $m := |\mathbb{F}^*|$  die Ordnung der multiplikativen Gruppe von  $\mathbb{F}$ . Dann gilt:

$$\log_m s = [\delta, \delta]_D + 1 - [\chi, \chi]_H - [\vartheta, \vartheta]_{E_\Phi} .$$

**Beweis.** Sei  $C_X := \mathbf{C}_{\mathrm{GL}_n(\mathbb{F})}(X)$  für  $X \in \{D, H, E_\Phi\}$ . Da  $\delta$  multiplizitätenfrei und  $\mathbb{F}$  ein Zerfällungskörper für  $H$  und  $E_\Phi$  ist, folgt nach dem Lemma von Schur, dass  $C_D$  ein direktes Produkt von  $[\delta, \delta]_D$  isomorphen Kopien der zyklischen Gruppe  $\mathbb{F}^*$  ist. Insbesondere ist  $C_D$  abelsch und für die beiden Untergruppen  $C_H, C_{E_\Phi} \leq C_D$  gilt deshalb

$$C_H R_i C_{E_\Phi} = C_H C_{E_\Phi} R_i \quad \text{für alle } i = 1, 2, \dots, s$$

und  $C_H C_{E_\Phi} = C_{E_\Phi} C_H$ . Also ist auch  $C_H C_{E_\Phi}$  eine Untergruppe von  $C_D$ , und zwar eine mit Index

$$s = |C_D : C_H C_{E_\Phi}| = \frac{|C_D| \cdot |C_H \cap C_{E_\Phi}|}{|C_H| \cdot |C_{E_\Phi}|} . \quad (\text{A})$$

Hierbei wissen wir schon, dass  $\log_m |C_D| = [\delta, \delta]_D$ ; ebenso liefert das Lemma von Schur jedoch  $\log_m |C_H| = [\chi, \chi]_H$  und  $\log_m |C_{E_\Phi}| = [\vartheta, \vartheta]_{E_\Phi}$ , denn mit  $\delta$  sind

selbstverständlich auch  $\chi$  und  $\vartheta$  multiplizitätenfrei. Die Behauptung ergibt sich demnach durch Logarithmieren der beiden Seiten von Gleichung (A) zur Basis  $m$ , falls  $|C_H \cap C_{E_\Phi}| = m$ .

Um dies zu zeigen, sei  $G := \langle H, E_\Phi \rangle$ . Angenommen, der natürliche  $\mathbb{F}G$ -Modul  $\mathbb{F}^n$  besäße einen nichttrivialen  $G$ -invarianten Submodul  $W$ .

Dann wäre der zu  $W \downarrow_H$  korrespondierende Charakter  $\chi_0 \in \text{Char}_{\mathbb{C}}(H)$  ein echter Konstituent von  $\chi$ , der zu  $W \downarrow_{E_\Phi}$  korrespondierende Charakter  $\vartheta_0 \in \text{Char}_{\mathbb{C}}(E_\Phi)$  ein echter Konstituent von  $\vartheta$  und das Paar  $(\chi_0, \vartheta_0)$  über  $D$  kompatibel — im Widerspruch zur Minimalität von  $(\chi, \vartheta)$ !

Folglich operiert  $G$  irreduzibel auf  $\mathbb{F}^n$ , weshalb  $\mathbf{C}_{\text{GL}_n(\mathbb{F})}(G) = C_H \cap C_{E_\Phi}$  nach dem Lemma von Schur tatsächlich nur aus den  $m$  skalaren Matrizen in  $\text{GL}_n(\mathbb{F})$  besteht.  $\square$

Vor dem Hintergrund von Lemma 2.2.5 ist klar, wie man die Charakteristik  $p$  bei praktischen Anwendungen des Michler-Algorithmus zunächst wählen wird: *minimal* unter all den Primzahlen in  $P$  derart, dass  $\mathbb{F} := \text{GF}(p)$  ein Zerfällungskörper für alle irreduziblen Konstituenten von  $\chi$  und  $\vartheta$  ist. Diese Vorgehensweise minimiert  $s$  und damit den Aufwand für

#### **Schritt 4c**

Setze  $\mathfrak{G}(\Phi) := \emptyset$ .

**Für**  $i \in \{1, 2, \dots, s\}$  :

Setze  $G_i := \langle H, E_\Phi^{R_i} \rangle$ .

**Für** zufällig ausgewählte  $g \in G_i$  :

Berechne die maximale 2-Potenz, welche in  $\text{ord}(g)$  aufgeht, und prüfe so, ob eine 2-Sylowuntergruppe von  $G_i$  isomorph zu  $S$  sein kann.

**Falls**  $G_i$  diesen 2-Sylowuntergruppentest bestanden hat : Setze  $\mathfrak{G}(\Phi) := \mathfrak{G}(\Phi) \cup \{G_i\}$ .

**Für**  $G \in \mathfrak{G}(\Phi)$  : Führe jeden der noch folgenden Schritte aus ...

In allen bisherigen Experimenten (siehe Abschnitt 2.3 für eine Übersicht) hat sich der 2-Sylowuntergruppentest als ein extrem scharfes Eliminationskriterium bewährt. Die Mächtigkeit der Menge  $\mathfrak{G}(\Phi)$  ist daher üblicherweise viel kleiner als  $s$ .

### 2.2.6 Von Matrixgruppen zu Permutationsgruppen

Das jetzt noch ausstehende Restprogramm filtert sämtliche Elemente aus  $\mathfrak{G}(\Phi)$ , die einfach sind und  $H$  als Zentralisator der 2-zentralen Involution  $z$  beherbergen.

#### **Schritt 5**

Berechne eine treue Permutationsdarstellung  $\pi$  von  $G$ .

Leider lässt sich in der Regel kaum vorhersagen, ob eine zu konstruierende Permutationsdarstellung treu sein wird oder nicht. Im Anschluss an eine entsprechende, bisweilen durchaus aufwendige Rechnung besteht allerdings selbst im Fall  $\text{Kern } \pi > \mathbf{1}_G$  kein Grund, gleich die Segel zu streichen: Die Matrixgruppe  $G$  ist dann zwar gewiss nicht einfach, scheidet als Lösung also prinzipiell aus; solange aber wenigstens  $\text{Kern } \pi \cap H = \mathbf{1}_G$  gilt, bleibt mit der Permutationsgruppe  $\pi(G) \geq \pi(H) \cong H$  ein Reservekandidat im Rennen.

**Schritt 6**

Berechne eine konkrete Charaktertafel für die Gruppe  $\pi(G)$ .  
Entscheide anhand dieser Tafel

- ob  $\pi(G)$  einfach ist und
- ob  $\pi(H) = \mathbf{C}_{\pi(G)}(\pi(z))$ .

**Ende**

Zweifellos zählt das Bestimmen einer Charaktertafel nicht unbedingt zu den effizientesten Methoden, um die Frage nach der Einfachheit einer Gruppe zu beantworten. Wann immer die Antwort negativ ausfällt, können wir einer konkreten Charaktertafel neben dieser Information jedoch auch prompt Erzeuger für einen nichttrivialen Normalteiler entnehmen.

## 2.3 Uniforme Existenzbeweise für 25 sporadische Gruppen

Wie G. O. Michler in [30] gezeigt hat, treten mit Ausnahme der Mathieu-Gruppe  $M_{11}$  alle bekannten sporadischen einfachen Gruppen als Lösung spezieller Instanzen des am Ende von Abschnitt 2.1 beschriebenen Einbettungsproblems auf. Dadurch ergibt sich nun offenbar die Möglichkeit, diese Gruppen mit Hilfe eines einheitlichen Verfahrens zu konstruieren, indem wir den Michler-Algorithmus mit der jeweils passenden Eingabegruppe  $H$  starten.

Am Institut für Experimentelle Mathematik der Universität Essen wurden so bis zum Zeitpunkt der Drucklegung Existenzbeweise für die folgenden sporadischen einfachen Gruppen geführt bzw. in Angriff genommen:

**Janko-Gruppen.** Ausgehend von einer kanonischen Permutationsdarstellung des direkten Produkts  $2 \times A_5$  gelang es G. O. Michler und M. K. [22], die kleinste Janko-Gruppe  $J_1$  (vergleiche [19]) als Untergruppe in  $GL_7(11)$  wiederzufinden.

Genau wie Z. Janko [20] selbst, trifft auch der Michler-Algorithmus über der zerfallenden Erweiterung  $2_-^{1+4} : A_5$  auf zwei verschiedene einfache Gruppen:  $J_2 \leq GL_{14}(11)$  und  $J_3$  als Bild ihrer dreifachen Überlagerung  $3J_3 \leq GL_{18}(31)$  unter einer Permutationsdarstellung mit zyklischem Kern der Ordnung 3. Weitere Details sind in [23] nachzulesen.

Die wesentlichen, sprich maschinell kritischen Teilschritte auf dem Weg zu einem Existenzbeweis für die größte Janko-Gruppe  $J_4$  (vergleiche [21]) haben M. Weller [44] und G. Cooperman et al. [10] bereits erledigt. Ebenfalls abgeschlossen, aber bislang noch undokumentiert ist die Berechnung kompatibler Paare (M. Weller). Auf die Bestimmung einer konkreten Charaktertafel für  $J_4$  wird ein Beispiel in Kapitel 3 näher eingehen.

**Held-Gruppe  $He$  und  $M_{24}$ .** Das zweite Paar sporadischer einfacher Gruppen mit übereinstimmendem Zentralisator einer 2-zentralen Involution hat W. Lempken [26] untersucht. Sein Experiment demonstriert unter anderem, dass es zu einer Isomorphieklasse von Erweiterungsgruppen  $E_\Phi$  eventuell *verschiedene* Einbettungen  $\mu_1, \mu_2 : D \hookrightarrow E_\Phi$  geben kann, die das Diagramm in Bedingung (c) von **Schritt 2** kommutieren lassen.

**Rudvalis-Gruppe Ru.** Sowohl D. Parrot [35] als auch S. B. Assa [1] haben Charakterisierungen der Rudvalis-Gruppe formuliert — über den Zentralisator einer 2-zentralen Involution bzw. über die Struktur einer 2-Sylowuntergruppe. Beide benutzen die von Parrot aufgestellte endliche Präsentation einer 2-Sylowuntergruppe innerhalb einer „Gruppe vom Typ Ru“.

Der erste Abschnitt von Kapitel 5 beschreibt, wie aus dieser Präsentation ein gemäß [35] geeigneter Zentralisator  $H$  als Eingabe für den Michler-Algorithmus konstruiert wird. Nachdem sich im weiteren Verlauf zeigt, dass die Bedingung  $\text{ggT}(p, |H||E_\Phi|) = 1$  an die Charakteristik  $p$  mit Rücksicht auf die zeitliche Durchführbarkeit von Schritt 4c nicht haltbar ist, gelangen wir auf dem Umweg über eine Diskussion der 5-modularen Darstellungen von  $H \cong 2^{5+6} : S_5$  schließlich zu  $\text{Ru} \leq \text{GL}_{133}(5)$ .

Nebenbei bemerkt fällt spätestens mit diesem Beispiel auch die Vermutung, der Michler-Algorithmus würde stets im Endergebnis  $G$  maximale Untergruppen  $E_\Phi$  produzieren.

**O’Nan-Gruppe ON.** Einem konstruktiven Zugriff am hartnäckigsten widersetzt hat sich bisher die sporadische einfache Gruppe ON. W. Lempken war mit Hilfe von GAP [39] in der Lage nachzurechnen, dass die Restriktion der kleinsten 31-modularen Darstellung von ON auf den Involutionenzentralisator  $H \cong 4_2L_3(4) : 2_1$  nicht multiplizitätenfrei ist. Günstiger sieht die Ausgangssituation hingegen bei der dreifachen Überlagerung 3ON aus, für die in [27] ein neuer Existenzbeweis angegeben wurde.

**Lyons-Gruppe Ly.** Mit  $\text{Ly} \leq \text{GL}_{111}(5)$  konnten G. O. Michler, K. Waki und M. Weller [31] zuletzt die größte Gruppe im Rahmen der laufenden Versuchsreihe konstruieren. Dieses Resultat komplettiert übrigens die Analyse aller sporadischen einfachen Gruppen, die nicht in M, dem so genannten Monster, enthalten sind.

## Kapitel 3

# Konkrete Charaktertafeln

Herkömmliche Anwendungen leiten aus den Daten einer Charaktertafel meist nur Aussagen ab, die für alle endlichen Gruppen mit ebendieser Tafel, speziell also für sämtliche Mitglieder einer Isomorphieklasse gleichermaßen gültig sind. Das vorangegangene Kapitel hat mehrere Situationen aufgezeigt, in denen irreduzible  $\mathbb{C}$ -Charaktere an gewissen „Stellen“, nämlich konkreten Gruppenelementen, als Funktion ausgewertet werden müssen. Hierzu bedarf es nicht bloß einer theoretisch konsistenten sondern auch einer *effektiv nachvollziehbaren* und jederzeit *exakt rekonstruierbaren* Verbindung zwischen den Konjugiertenklassen der betrachteten Gruppe und den Spalten ihrer Charaktertafel.

Algorithmen zur Berechnung eines hinreichend standardisierten Repräsentantensystems für die Konjugiertenklassen einer endlichen Gruppe stehen deshalb zunächst im Brennpunkt jeder weiteren Überlegung.

Lediglich am Rande streifen werden wir dagegen den Themenkomplex der computeralgebraischen Methoden zur Bestimmung aller irreduziblen  $\mathbb{C}$ -Charaktere einer endlichen Gruppe. Die hierbei vorgeschlagene Prozedur vermag dem klassischen Algorithmus von J. D. Dixon [12] und G. J. A. Schneider [38] in Fällen, wo dessen direkter Einsatz an die Kapazitätsgrenzen moderner Hardware stößt, entscheidend auf die Sprünge zu helfen und — wie ein Beispiel belegt — bisweilen sogar die gesamte Arbeit abzunehmen.

### 3.1 Präzisierung der fundamentalen Begriffe

Sei  $G$  eine endliche Gruppe und  $\mathcal{S}$  die Menge ihrer Konjugiertenklassen. Eine (**gewöhnliche**) **Charaktertafel**  $\Theta$  von  $G$  ist formal nichts anderes als eine gemeinsame Wertetabelle für eine Menge  $\mathcal{Z}$  von im Wesentlichen auf  $\mathcal{S}$  erklärten Abbildungen. Obligatorisch zählen dazu **Klassenfunktionen**  $G \rightarrow \mathbb{C}$ , denn  $\mathcal{Z}$  muss mindestens die Menge  $\text{Irr}_{\mathbb{C}}(G)$  der irreduziblen  $\mathbb{C}$ -Charaktere  $\chi_1 = \mathbb{1}_G, \chi_2, \dots, \chi_{|\mathcal{S}|}$  von  $G$  umfassen. Darüber hinaus enthält  $\mathcal{Z}$  optional:

- **Klasseninvarianten**  $G \rightarrow \mathbb{N}$ , wie die Elementordnung  $\text{ord}(x)$ , die Länge der Konjugiertenklasse  $(x)^G$  oder die Ordnung des Zentralisators  $\mathbf{C}_G(x)$ ;
- **Potenzabbildungen**  $\mathcal{S} \rightarrow \mathcal{S}$ ,  $(x)^G \mapsto (x^p)^G$ , idealerweise zu allen für die Gruppe  $G$  relevanten Primzahlexponenten  $p \leq \max\{\text{ord}(g) \mid g \in G\}$ ;
- **Fusionen**, jeweils von  $\mathcal{S}$  in die Menge der Konjugiertenklassen einer Obergruppe zu  $G$ .

Während die Zuordnung zwischen den Elementen von  $\mathcal{Z}$  und den Zeilen von  $\Theta$  inhärent gegeben und somit stets eindeutig ist, unterscheiden wir prinzipiell zwei Arten der Zuordnung zwischen den Elementen von  $\mathcal{S}$  und den Spalten von  $\Theta$ .

**Definition 3.1.1** (Konkretheit und Abstraktheit von Charaktertafeln)

Sei  $G$  eine endliche Gruppe.

Eine Charaktertafel  $\Theta$  von  $G$  heißt **konkret**, falls jede ihrer Spalten mit einem Vertreter der zugehörigen Konjugiertenklasse von  $G$  markiert ist. Ansonsten heißt  $\Theta$  **abstrakt**.

Neben den offensichtlichen Vorteilen, die eine konkrete Charaktertafel zu bieten hat, haftet ihr wenigstens auf den ersten Blick auch ein großer Nachteil an: Sie benötigt mehr Platz, unter für experimentelle Anwendungen typischen Umständen sogar sehr viel mehr Platz als eine abstrakte Version. Diesen Effekt beleuchten auch die folgenden Beispiele.

**Beispiel 3.1.2** Eine konkrete Charaktertafel für die symmetrische Gruppe  $S_4$ .

Gruppe $G = S_4$				$ G  = 2^3 \cdot 3 = 24$	
Klassenname :	1	$2_1$	$2_2$	3	4
Repräsentant :	()	$(1, 2)(3, 4)$	$(1, 2)$	$(1, 2, 3)$	$(1, 2, 3, 4)$
Klassenlänge :	1	3	6	8	6
2P :	1	1	1	3	$2_1$
3P :	1	$2_1$	$2_2$	1	4
$\chi_1$ :	1	1	1	1	1
$\chi_2$ :	1	1	-1	1	-1
$\chi_3$ :	2	2	0	-1	0
$\chi_4$ :	3	-1	1	0	-1
$\chi_5$ :	3	-1	-1	0	1

Allein durch das Weglassen der Repräsentantenzeile würde aus der vorliegenden konkreten Tafel eine abstrakte werden. Man beachte jedoch, dass dieser Prozess nicht unmittelbar reversibel ist: Gemäß einer ungeschriebenen Konvention sollte aus den Namen der einzelnen Konjugiertenklassen zwar wie hier die Ordnung ihrer Elemente hervorgehen, um aber etwa in  $G$  nicht konjugierte Involutionen  $t_1$  und  $t_2$  wieder den passenden Spalten zuzuweisen, kann auf die explizite Berechnung der Klassenlänge  $|(t_1)^G|$  oder  $|(t_2)^G|$  nicht verzichtet werden.

Da sich  $S_4$  als Permutationsgruppe auf nur vier Punkten darstellen lässt, findet garantiert jede beliebige Wahl von Konjugiertenklassenrepräsentanten Platz in der dafür vorgesehenen Zeile. Bei Gruppen, deren kleinste treue Permutationsdarstellung einen Grad  $> 20$  besitzt, sieht die Situation mit gleichem Schriftsatz schon erheblich unangenehmer aus, und erst recht würden Repräsentanten für die Konjugiertenklassen von Matrixgruppen eines Rangs  $> 10$  den Seitenspiegel sprengen.

Was auf dem Papier und in relativ geringem Maßstab noch wie ein rein ästhetisches Problem anmutet, führt auf einem Rechner im Rahmen ernsthaft interessanter Größenverhältnisse unweigerlich zu einem massiven Verbrauch von Speicherressourcen.

### Beispiel 3.1.3 Charaktertafeln in MAGMA und GAP.

Sowohl GAP [13], [39] als auch MAGMA [2] bieten ihren Benutzern eine Implementierung des einleitend bereits erwähnten Dixon-Schneider-Algorithmus. Jede damit bestimmte Charaktertafel ist konkret im Sinne von Definition 3.1.1, denn die Spalten einer solchen Tafel sind über programminterne Referenzen umkehrbar eindeutig mit den Elementen eines Vertretersystems für die Konjugiertenklassen der zugrunde liegenden Gruppe verlinkt. Bei einem Ausdruck der Tafel am Bildschirm allerdings wird diese Spaltenmarkierung komplett unterdrückt:

<pre> gap&gt; # Charaktertafel zu S_4 gap&gt; # berechnet mit GAP4 gap&gt; G := SymmetricGroup( 4 ); Sym( [ 1 .. 4 ] ) gap&gt; ctG := CharacterTable( G ); CharacterTable( Sym( [ 1 .. 4 ] ) ) gap&gt; Display( ctG ); </pre>	<pre> &gt; // Charaktertafel zu S_4 &gt; // berechnet mit MAGMA V2.7 &gt; G := SymmetricGroup( 4 ); &gt; ctG := CharacterTable( G ); &gt; ctG; </pre>
<pre> CT1 </pre>	<pre> Character Table of Group G ----- </pre>
<pre>       2  3  3  2  .  2       3  1  .  .  1  . </pre>	<pre> ----- Class    1  2  3  4  5 Size     1  3  6  8  6 Order    1  2  2  3  4 ----- p  =  2   1  1  1  4  2 p  =  3   1  2  3  1  5 ----- </pre>
<pre>       1a 2a 2b 3a 4a 2P 1a 1a 1a 3a 2a 3P 1a 2a 2b 1a 4a </pre>	
<pre> X.1      1  1  1  1  1 X.2      1  1 -1  1 -1 X.3      2  2  . -1  . X.4      3 -1 -1  .  1 X.5      3 -1  1  . -1 </pre>	<pre> X.1  +   1  1  1  1  1 X.2  +   1  1-1  1-1 X.3  +   2  2  0-1  0 X.4  +   3-1  1  0-1 X.5  +   3-1-1  0  1 </pre>

Beide Pakete berücksichtigen also die Existenz von Permutationsgruppen höheren Grades bzw. von Matrixgruppen entsprechend hohen Rangs und bringen platzsparend lediglich eine abstrakte Charaktertafel zur Anzeige.

Abgesehen von der Fähigkeit, Charaktertafeln für explizit gegebene Gruppen selber zu berechnen, besitzt GAP eine riesige Sammlung abstrakter Charaktertafeln. Vorwiegend aus dem Atlas [8] der einfachen endlichen Gruppen übernommen, auf Konsistenz geprüft und nötigenfalls korrigiert, besteht zwischen diesen Tafeln und den passenden Gruppen aus der GAP-Gruppenbibliothek momentan keinerlei Verbindung. Um eine derartige Beziehung zu etablieren, müssten sämtliche Einträge der Gruppenbibliothek um ein Konjugiertenklassenrepräsentantensystem ergänzt werden, was den durch eine GAP-Installation eingenommenen Plattenplatz deutlich in die Höhe schrauben würde.

Mit  $x := (1, 2)$  und  $y := (1, 2, 3, 4)$  sind etwa  $1, y^2, x, xy$  bzw.  $y$  Repräsentantenworte für die konjugierten Klassen  $1, 2_1, 2_2, 3$  bzw.  $4$  der Gruppe  $G := \langle x, y \rangle \cong S_4$  aus Beispiel 3.1.2. Doch wie kann solch ein Repräsentantensystem algorithmisch ermittelt werden?

Zwischen der Menge aller möglichen Worte in den fixierten Erzeugern einer Gruppe  $G$  und der Menge aller endlichen, an der Wurzel  $1_G$  beginnenden und wiederholungsfreien Pfade im vollständigen Wortbaum  $\mathcal{B}(G)$  existiert eine kanonische Bijektion:



Die Markierungen der in einem Pfad  $\mathcal{P}$  auftretenden Knoten ergeben von oben nach unten gelesen gerade das zu  $\mathcal{P}$  korrespondierende Wort  $w_{\mathcal{P}}$ . Umgekehrt ist ein Wort  $w$  von links nach rechts gelesen gleichermaßen die Wegbeschreibung für den zu  $w$  korrespondierenden Pfad  $\mathcal{P}_w$ .

Insbesondere durchlaufen wir daher tatsächlich die Gesamtheit der Worte aus  $\ell \geq 0$  Faktoren, wenn wir in  $\mathcal{B}(G)$  per Breitensuche (engl.: **breadth first search**, kurz BFS) nacheinander alle von der Wurzel  $1_G$  ausgehenden, wiederholungsfreien Pfade<sup>1</sup> der Länge  $\ell$  betrachten.

**Algorithmus 3.2.2** (kürzeste Repräsentantenworte, Version 1)

Sei  $G$  eine endliche Gruppe und die Teilmenge  $\{x_1, x_2, \dots, x_k\} \subseteq G$ ,  $k \in \mathbb{N}$ , ein fest gewähltes Erzeugendensystem für  $G$ .

**Schritt 1**

Initialisiere die Menge der gefundenen Repräsentantenworte  $W := \{1_G\}$ .

Initialisiere die Kontrollsumme  $c = \sum_{w \in W} |(w)^G| := 1$ .

Berechne  $m := |G|$ .

**Schritt 2**

**Solange**  $c \neq m$  :

Bestimme den gemäß BFS nächsten Pfad  $\mathcal{P}$  in  $\mathcal{B}(G)$ .

**Falls**  $w_{\mathcal{P}}$  in  $G$  zu keinem  $w \in W$  konjugiert ist :

Setze  $W := W \cup \{w_{\mathcal{P}}\}$ .

Inkrementiere  $c$  um  $|(w_{\mathcal{P}})^G| = m \cdot |\mathbf{C}_G(w_{\mathcal{P}})|^{-1}$ .

**Ende**

Eine Aussage über die wichtigsten Eigenschaften dieses Verfahrens macht

**Satz 3.2.3**

*Angewandt auf eine endliche Gruppe  $G$  mit Erzeugermenge  $X$  terminiert Algorithmus 3.2.2. Die resultierende Menge  $W$  ist dann ein Vertretersystem für die Konjugiertenklassen von  $G$ , und alle Repräsentantenworte  $w \in W$  sind von minimaler Länge bezüglich  $X$ .*

**Beweis.** Für  $|G| = 1$  ist die Behauptung trivial. Sei also  $|G| > 1$ .

Jedes Element von  $G$  kann wegen  $G = \langle X \rangle$  durch wenigstens einen Pfad in  $\mathcal{B}(G)$  dargestellt werden, und die Gleichung

$$c = \sum_{w \in W} |(w)^G|$$

ist eine Invariante des beschriebenen Algorithmus. Da sich der Wert von  $c$  niemals verringert, sondern genau dann steigt, wenn ein neuer Konjugiertenklassenrepräsentant  $w_{\mathcal{P}}$  gefunden wurde, muss  $c$  nach endlich vielen Iterationen gleich

---

<sup>1</sup>Streng genommen traversiert BFS die *Knoten* eines Baumes. Weil hier wie im Folgenden jedoch ausschließlich wiederholungsfreie Pfade behandelt werden, deren Anfangsknoten die Baumwurzel ist, legt die Wahl eines Endknotens immer schon einen ganzen *Pfad* eindeutig fest. Deshalb dürfen wir BFS auch als Traversierung der für uns relevanten Pfade interpretieren.

der Summe über die Längen aller Konjugiertenklassen von  $G$ , sprich gleich  $m$  sein. Folglich terminiert das Verfahren und liefert mit der Menge  $W$  bei regulärem Abbruch ein Vertretersystem.

Die BFS-Strategie garantiert die besagte Minimaleigenschaft der Worte in  $W$ .  $\square$

Entgegen den optimistischen Voraussetzungen dieses Abschnitts bereitet die Berechnung von Klassenlängen sowie der definitive Test zweier Elemente auf Konjugiertheit in Matrixgruppen praktisch unüberwindbare Schwierigkeiten. Und selbst für Permutationsgruppen zählen die genannten Operationen nicht eben zu den billigsten.

Mithin sind ein paar effizienzsteigernde Maßnahmen erforderlich, bevor wir das durch Algorithmus 3.2.2 ins Spiel gebrachte Backtracking-Prinzip für unsere Zwecke sinnvoll umsetzen können.

### 3.3 Konjugiertheitskriterien

Dass zwei Elemente einer Gruppe *nicht* konjugiert sind, lässt sich häufig mit sehr einfachen Mitteln beweisen. Unabhängig vom speziellen Universum, in dem die Gruppe lebt, also für Permutations- ganz genauso wie für Matrixgruppen stimmt bekanntlich

#### Lemma 3.3.1

Es sei  $G$  eine endliche Gruppe und  $g, h \in G$ . Dann gilt:

$$\text{ord}(g) \neq \text{ord}(h) \implies g \not\sim_G h ;$$

denn als Automorphismus muss jede Konjugation die Elementordnung respektieren.

Während die Umkehrung von Lemma 3.3.1 zum Beispiel durch  $g = (1, 2)$  und  $h = (1, 2)(3, 4)$  in  $G = S_4$  widerlegt wird, existieren gerade für die Konjugiertheit von Permutationen in den symmetrischen Gruppen bzw. von Matrizen in den generellen linearen Gruppen leicht auszuwertende Kriterien, die zugleich notwendig und hinreichend sind.

#### Definition 3.3.2 (universelle Konjugiertheit)

Sei  $\mathbb{F}$  ein Körper und  $n \in \mathbb{N}$ . Ferner sei  $G$  eine Untergruppe von  $S_n$  bzw. von  $\text{GL}_n(\mathbb{F})$ .

Zwei Elemente  $g, h \in G$  heißen **zueinander universell konjugiert**, in Zeichen

$$g \sim h ,$$

wenn sie in  $S_n$  bzw. in  $\text{GL}_n(\mathbb{F})$  konjugiert sind. Für ein Element  $g \in G$  heißt die Menge

$$(g)_G := \{x \in G \mid g \sim x\}$$

die **universelle Konjugiertenklasse von  $g$  in  $G$** .

Konjugiertheit in einer Permutations- oder Matrixgruppe  $G$  impliziert universelle Konjugiertheit. Von entscheidender Bedeutung ist aber, dass zwei Elemente  $g, h \in G$ , die nicht universell konjugiert sind, erst recht nicht in  $G$  konjugiert sein können. Die universellen Konjugiertenklassen von  $G$  bilden demnach eine gewisse Approximation der Konjugiertenklassen von  $G$ . In den nächsten beiden Unterabschnitten erwartet uns primär eine Sammlung der elementaren algebraischen Werkzeuge zur Konstruktion dieser Näherung. Gegebenenfalls wollen wir jedoch auch kurz erörtern, welche Algorithmen uns zu noch genaueren Aussagen befähigen.

### 3.3.1 Zur Konjugiertheit von Permutationen

Seien  $g$  und  $h$  zwei Permutationen vom Grad  $n \in \mathbb{N}$ . Beim Konjugieren von  $g$  mit  $h$  werden in sämtlichen Zykeln von  $g$  alle Einträge durch ihr jeweiliges Bild unter  $h$  ersetzt. Auf exakt diesem Zusammenhang beruht die folgende Charakterisierung der universellen Konjugiertheit von Elementen einer Permutationsgruppe.

#### Lemma 3.3.3

*Es sei  $G$  eine Untergruppe der symmetrischen Gruppe  $S_n$ ,  $n \in \mathbb{N}$ . Dann gilt für  $g, h \in G$ :*

$$g \sim h \iff g \text{ und } h \text{ besitzen dieselbe Zykelstruktur.}$$

Sogar für Permutationen auf mehr als  $10^6$  Punkten lässt sich unter MAGMA bzw. GAP relativ schnell die Zykelstruktur ermitteln. Daher stellt unsere ursprüngliche Frage, ob  $g$  und  $h$  aus Lemma 3.3.3 nun in  $G$  konjugiert sind oder nicht, nur dann ein wirklich kritisches Problem dar, wenn  $g$  und  $h$  universell konjugiert sind. Im Fall von Permutationsgruppen kann diese Aufgabe dennoch effizient algorithmisch bewältigt werden.

#### □ Backtracking, zum Zweiten

Das klassische Entscheidungsverfahren gehört aus rein methodischer Sicht zu einer mächtigen Algorithmenfamilie, die von G. Butler in [4] und in Kapitel 11 von [5] detailliert beschrieben wurde. Wie all seine Verwandten gründet es sich auf die von C. C. Sims [40], [41] entwickelten Konzepte der *Basis* und der *starken Erzeugermenge* für eine Permutationsgruppe  $G$ .

Sei  $\Omega$  die Punktmenge, auf der  $G$  operiert. Zu jedem vorgegebenen Bildtupel  $B'$  über  $\Omega$  einer geordneten Basis  $B$  von  $G$  gibt es höchstens ein Element  $x \in G$  mit  $B^x = B'$ . Anhand der Schreivervektoren zu den Basisorbits von  $G$  kann dieses  $x$  entweder bestimmt oder der Beweis erbracht werden, dass kein  $x \in G$  die Basis  $B$  in  $B'$  überführt.

Betrachten wir zwei universell konjugierte Elemente  $g, h \in G$ . Liegt ein Basispunkt  $\beta \in B$  in einem  $g$ -Zykel der Länge  $\ell$ , so kommen als Bild von  $\beta$  unter einem  $y \in G$  mit  $g^y = h$  freilich bloß solche Punkte  $\beta'$  in Frage, die in  $h$ -Zykeln der Länge  $\ell$  anzutreffen sind.

Um herauszufinden, ob  $g \sim_G h$  gilt, wird dasselbe Argument einfach auf die gesamte Basis erweitert: Im Modus „trial-and-error“ durch die Stabilisatorenkette von  $G$  bezüglich  $B$  laufend, wähle der Reihe nach Bilder  $\gamma_1, \gamma_2, \dots$  für die Basispunkte  $\beta_1, \beta_2, \dots$  und konstruiere dazu schrittweise den potentiellen Konjugator

$$y = y_1 \cdot y_2 \cdot \dots \in G, \quad \text{so dass } \beta_1^y = \gamma_1, \beta_2^y = \gamma_2, \text{ usw.}$$

Wann immer schließlich ein komplettes Bildtupel  $B' = (\gamma_1, \gamma_2, \dots, \gamma_{|B|})$  sowie ein  $y \in G$  mit der Eigenschaft  $B^y = B'$  aufgebaut wurde, teste ob  $g^y = h$ . Falls ja, folgt  $g \sim_G h$ ; der Algorithmus bricht dann ab. Sind nach endlich vielen Fehlversuchen alle zulässigen Alternativen erschöpft, zeigt dies die Nichtexistenz eines Konjugators in  $G$ , also  $g \not\sim_G h$ .

#### □ Geordnete Partitionen

Eine fundamentale Optimierung des oben skizzierten Verfahrens stammt von J. S. Leon [29]. Statt die Aktion möglicher Konjugatoren  $y \in G$  lediglich gegenüber einer Basis zu kontrollieren, sollte fortan ihre Wirkung auf gewisse *geordnete Partitionen* von  $\Omega$  ins Blickfeld rücken.

Sei  $n := |\Omega|$  der Grad von  $G$ , und seien  $g, h \in G$  wieder universell konjugiert. Durch spezifisch gewählte **Verfeinerungsprozesse** werden die trivialen Partitionen  $\Pi_0 = \Sigma_0 = (\Omega)$  einerseits Zelle für Zelle in zwei diskrete Partitionen

$$\Pi_n = (\omega_1 | \omega_2 | \cdots | \omega_n) \quad \text{und} \quad \Sigma_n = (\omega'_1 | \omega'_2 | \cdots | \omega'_n)$$

aufgesplittet. Ein Verfeinerungsprozess ist dabei ein Paar  $(\mathfrak{L}, \mathfrak{R})$  von Partitionsverfeinerungen, die sich mit der Anwendung jedes beliebigen Konjugators  $y \in G$  in folgendem Sinne vertragen:

$$g^y = h \quad \text{und} \quad \Pi^y = \Sigma \quad \implies \quad \mathfrak{L}(\Pi)^y = \mathfrak{R}(\Sigma),$$

wo  $\Pi$  und  $\Sigma$  geordnete Partitionen von  $\Omega$  bezeichnen.

Andererseits muss für alle Übergänge von  $\Pi_d$  zu  $\Pi_{d+1}$  bzw. von  $\Sigma_d$  zu  $\Sigma_{d+1}$ ,  $0 \leq d < n$ , jeweils geprüft werden, ob  $\Pi_{d+1}$  nach wie vor noch durch ein  $y \in G$  auf  $\Sigma_{d+1}$  abgebildet werden kann. Wann immer es schließlich gelingt, bis zu diskreten Partitionen abzusteigen, teste, ob für das entsprechende  $y \in G$  mit  $\Pi_n^y = \Sigma_n$  auch  $g^y = h$  gilt. Falls ja, folgt  $g \sim_G h$ , und die Suche war erfolgreich. Ansonsten storniere die letzten Splits von  $\Sigma_n$  und fahre mit eventuellen Alternativen fort. Ist selbst das nicht mehr möglich, zeigt dies die Nichtexistenz eines Konjugators in  $G$ , also  $g \not\sim_G h$ .

Wie sein Vorgänger lässt sich der gesamte Algorithmus als Backtracking-Verfahren über einem Baum implementieren: „The node  $\Sigma_d$  [at depth  $d$ ] represents a right coset  $G_{\Pi_d}t$ , where  $t \in G$  such that  $\Pi_d^t = \Sigma_d$  may hold. The sons of node  $\Sigma_d$  represent possible images of  $\Sigma_{d+1}$  under elements of  $G_{\Pi_d}t$ . A leaf node corresponds to an element of  $G$ .“<sup>2</sup>

Aufgrund der Tatsache, dass nun aber das Bild einer ganzen geordneten Partition von  $\Omega$  über die Eignung eines Elements  $y \in G$  als Konjugator entscheidet — und nicht mehr nur das Bild einer Basis von  $G$  — werden die „Sackgassen“ des neuen Baumes im Mittel erheblich früher erkannt und eliminiert.

### 3.3.2 Zur Konjugiertheit von Matrizen

In der Sprache der Linearen Algebra heißen universell konjugierte Matrizen **ähnlich**. Aufsteigend sortiert nach dem rechnerischen Aufwand, den ihre einmalige Auswertung kostet, fasst das folgende Lemma die gebräuchlichsten Kriterien für Ähnlichkeit von Matrizen zusammen:

#### Lemma 3.3.4

Es sei  $\mathbb{F}$  ein Körper und  $G$  eine Untergruppe der generellen linearen Gruppe  $\text{GL}_n(\mathbb{F})$ ,  $n \in \mathbb{N}$ . Dann gelten für  $g, h \in G$ :

- (a)  $g \sim h \implies \text{Spur}(g) = \text{Spur}(h);$
- (b)  $g \sim h \implies \text{Det}(g) = \text{Det}(h);$
- (c)  $g \sim h \iff \text{RKF}(g) = \text{RKF}(h),$

wobei  $\text{RKF}(m)$  die rationale kanonische Form einer Matrix  $m \in \text{GL}_n(\mathbb{F})$  bezeichne.

---

<sup>2</sup>Zitat J. S. Leon [29], Seite 542.

Über endlichen Primkörpern  $\mathbb{F}$  einer Charakteristik  $\leq 199$  beträgt die Laufzeit der einschlägigen MAGMA-Funktion `RationalForm( m )` auf einem modern ausgerüsteten Arbeitsplatzrechner circa eine CPU-Sekunde, solange der Rang  $n \leq 200$  bleibt. Für größer dimensionierte Matrizen oder solche mit Einträgen aus algebraischen Erweiterungen endlicher Körper wird die Berechnung rationaler kanonischer Formen schnell eine teure Angelegenheit.

Bei annähernd gleichbleibendem Rechenaufwand nimmt die Güte der notwendigen Kriterien Spur und Determinante hingegen stark zu, je mehr Elemente ihr Wertebereich  $\mathbb{F}$  besitzt.

Analog zum Unterabschnitt über Permutationen wäre jetzt die Frage zu stellen, auf welche Weise wir für zwei universell konjugierte Matrizen  $g, h \in G \leq \mathrm{GL}_n(\mathbb{F})$  entscheiden können, ob  $g \sim_G h$  oder  $g \not\sim_G h$ . Leider existiert zur Lösung dieses Problems jedoch bislang kein generell praktikabler Algorithmus.

Das mag zunächst verwundern, denn gerade Matrizen über endlichen Körpern verhalten sich ja im Grunde nicht wesentlich anders als Permutationen; statt auf einer Menge von Ziffern operieren sie eben auf einer Menge von Vektoren oder Untervektorräumen. Ein Transfer der für Permutationsgruppen benutzten und bewährten Konzepte ist daher theoretisch denkbar. Praktisch scheitert diese Übertragung bereits für Matrixgruppen  $G$  von kleinem Rang  $n$  an der Schwierigkeit, *automatisch* eine treue Permutationsdarstellung von  $G$  zu finden. Die einzige garantierte sichere Wahl ist die Identifikation des zugrunde liegenden Vektorraums  $\mathbb{F}^n$  mit der Ziffernmenge  $\{1, 2, \dots, |\mathbb{F}|^n\}$ , also die natürliche Einbettung von  $G$  in die symmetrische Gruppe  $S_{|\mathbb{F}|^n}$ .

Aus einer Matrixgruppe vom Rang 10 über dem Körper  $\mathrm{GF}(7)$  wird damit aber zum Beispiel eine Permutationsgruppe vom Grad  $7^{10} = 282475249$ , das heißt allein das Abspeichern eines Erzeugers würde gut ein Gigabyte Platz beanspruchen.

### 3.3.3 Zur Konjugiertheit von Worten in Erzeugern

Im Vergleich deutlich kompakter zu handhaben ist ein Gruppenelement, wenn es als Wort in den Erzeugern der betreffenden Gruppe vorliegt. Um zwei derartige Worte auf Konjugiertheit zu testen, müssen in der Regel allerdings beide ausmultipliziert werden. Nur unter besonderen Voraussetzungen können wir uns diesen Schritt sparen.

#### Definition 3.3.5 (zyklischer Shift)

Sei  $G = \langle x_1, x_2, \dots, x_k \rangle$ ,  $k \in \mathbb{N}$ , eine endliche Gruppe, und sei  $w = w(x_1, x_2, \dots, x_k)$  ein Wort in den Erzeugern von  $G$ .

Ein Wort  $s = s(x_1, x_2, \dots, x_k)$  heißt ein **zyklischer Shift von  $w$** , falls es sich so in zwei Teilworte  $u$  und  $v$  zerlegen lässt, dass  $s = uv$  und  $w = vu$ .

#### Lemma 3.3.6

Es sei  $G = \langle x_1, x_2, \dots, x_k \rangle$ ,  $k \in \mathbb{N}$ , eine endliche Gruppe und  $w = w(x_1, x_2, \dots, x_k)$  ein Wort in den Erzeugern von  $G$ . Dann gilt:

Jeder zyklische Shift von  $w$  ist in  $G$  zu  $w$  konjugiert.

**Beweis.** Sei  $s = s(x_1, x_2, \dots, x_k)$  ein zyklischer Shift von  $w$ . Gemäß Definition 3.3.5 existieren dann Teilworte  $u, v$  von  $s$  mit  $s = uv$  und  $w = vu$ . Dies impliziert

$$s^u = u^{-1}su = u^{-1}uvu = vu = w,$$

respektive  $s \sim_G w$ , weil  $u$  ein Wort in den Erzeugern von  $G$  ist. □

Die Umkehrung der Aussage von Lemma 3.3.6 ist im Allgemeinen falsch. Ein Gegenbeispiel liefert uns einmal mehr die symmetrische Gruppe  $G = S_4$ : Für die Erzeuger  $x := (1, 2)$  und  $y := (1, 2, 3, 4)$  gilt zwar  $xyx \sim_G yxy$ , doch diese beiden Worte sind offensichtlich keine zyklischen Shifts voneinander.

Dessen völlig ungeachtet erlaubt das Resultat immerhin eine beträchtliche Steigerung der Effizienz von Algorithmus 3.2.2.

### 3.4 Beschleunigte Breitensuche

Mit einem Wort  $w$  in den Erzeugern einer Gruppe  $G$  enthält der vollständige Wortbaum  $\mathcal{B}(G)$  natürlich auch alle zyklischen Shifts  $s$  von  $w$ . Deshalb erledigt eine BFS-Traversierung von  $\mathcal{B}(G)$  nach Lemma 3.3.6 sehr viel mehr Arbeit als zum Aufsammeln je eines Repräsentanten der verschiedenen Konjugiertenklassen von  $G$  unbedingt notwendig wäre: Unabhängig davon, ob  $w$  selber eine bis dahin unbekannte Klasse vertritt oder nicht, die weitere Untersuchung zyklischer Shifts von  $w$  ist in jedem Falle überflüssig.

#### 3.4.1 Redundanzbereinigung auf Wortebene

Im Folgenden bezeichne  $\mathcal{W}(G)$  die Menge aller Worte in den Erzeugern einer Gruppe  $G$ . Vermöge einer geeigneten Ordnung auf  $\mathcal{W}(G)$  kann die Analyse zyklischer Shifts optimal organisiert werden.

**Definition 3.4.1** (längen-lexikographische Ordnung)

Sei  $G$  eine endliche Gruppe und die Teilmenge  $\{x_1, x_2, \dots, x_k\} \subseteq G$ ,  $k \in \mathbb{N}$ , ein fest gewähltes Erzeugendensystem für  $G$ . Ferner symbolisiere  $\preceq$  die durch  $x_1 \prec x_2 \prec \dots \prec x_k$  induzierte lexikographische Ordnung auf  $\mathcal{W}(G)$ .

Für zwei beliebige Worte  $u = u(x_1, x_2, \dots, x_k)$  und  $v = (x_1, x_2, \dots, x_k)$  aus  $\mathcal{W}(G)$  gelte

$$u \sqsubseteq v \quad :\Longleftrightarrow \quad |u| < |v| \quad \text{oder} \quad |u| = |v| \quad \text{und} \quad u \preceq v. \quad (\text{B})$$

Dann ist  $\sqsubseteq$  eine totale Ordnungsrelation auf  $\mathcal{W}(G)$  und heißt die **längen-lexikographische Ordnung**.

Wir notieren eine unmittelbar aus (B) folgende, aber extrem wichtige Eigenschaft der längen-lexikographischen Ordnung:

**Satz 3.4.2**

*Es sei  $G = \langle x_1, x_2, \dots, x_k \rangle$ ,  $k \in \mathbb{N}$  eine endliche Gruppe. Dann gilt:*

*Die BFS-Traversierung des vollständigen Wortbaums  $\mathcal{B}(G)$  durchläuft die Menge  $\mathcal{W}(G)$  in längen-lexikographisch aufsteigender Reihenfolge.*

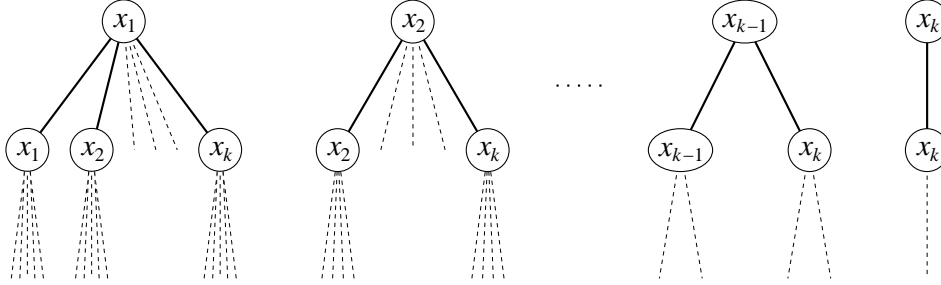
Hieraus ergibt sich wiederum eine simple Verfahrensvorschrift, um sämtliche zyklischen Shifts eines schon geprüften Wortes automatisch zu überspringen: Ziehe ein Wort  $w$  *genau dann* für die Rolle eines Konjugiertenklassenvertreters in Betracht, *wenn* kein zyklischer Shift von  $w$  (längen-)lexikographisch kleiner ist als  $w$  selber.

Zyklische Shifts bloß zu erkennen und von tiefergehenden Tests auszuklammern stellt per se gewiss keine ideale Lösung dar. Am effektivsten wäre es zweifellos, auf einem absolut „shift-freien“ Wortbaum agieren zu können. Eine solche Situation lässt sich zumindest annähernd erreichen.

Für ein beliebiges Wort  $w$ , dessen lexikographisch kleinster Faktor etwa der Erzeuger  $x$  ist, bleibt nämlich dem (längen-)lexikographisch minimalen zyklischen Shift von  $w$  gar nichts anderes übrig als mit  $x$  zu beginnen. Diese Überlegung motiviert

**Definition 3.4.3** (Erzeuger-Wortbaum, shiftreduzierter Wortbaum)

Sei  $G$  eine endliche Gruppe und die Teilmenge  $\{x_1, x_2, \dots, x_k\} \subseteq G$ ,  $k \in \mathbb{N}$ , ein fest gewähltes, lexikographisch aufsteigend indiziertes Erzeugendensystem für  $G$ . Ferner sei  $1 \leq i \leq k$ . Der unendlich tiefe,  $(k - i + 1)$ -näre Baum  $\mathcal{B}(x_i)$  mit Wurzel  $x_i$ , in dem die Söhne eines jeden Knotens sukzessive von links nach rechts mit  $x_i, x_{i+1}, \dots, x_{k-1}$  bzw.  $x_k$  markiert sind, heißt der **Wortbaum über  $x_i$**  oder einfach kurz der  **$x_i$ -Wortbaum**.



Der unendlich tiefe Baum  $\mathcal{R}(G)$  mit Wurzel  $1_G$ , an der sukzessive von links nach rechts die Bäume  $\mathcal{B}(x_1), \mathcal{B}(x_2), \dots, \mathcal{B}(x_k)$  hängen, heißt der **shiftreduzierte Wortbaum von  $G$** .

Mit einem Wort  $w$  enthält der shiftreduzierte Wortbaum nurmehr diejenigen zyklischen Shifts von  $w$ , welche denselben Anfangsfaktor wie  $w$  besitzen — daher der Name.

Wieviel man durch eine Verlagerung der Repräsentantensuche von  $\mathcal{B}(G)$  nach  $\mathcal{R}(G)$  wirklich gewinnt, zeigt der quantitative Vergleich zwischen den Mengen der jeweils zu untersuchenden Worte: Während sich aus  $k \geq 2$  Erzeugern insgesamt, sprich im vollständigen Wortbaum,

$$b(k, m) := \sum_{d=0}^m k^d = \frac{k^{m+1} - 1}{k - 1}$$

verschiedene Worte der maximalen Länge  $m$  zusammensetzen, kommen davon lediglich

$$r(k, m) := 1 + \sum_{i=1}^k \sum_{d=0}^{m-1} i^d = 1 + m + \sum_{i=2}^k \frac{i^m - 1}{i - 1}$$

im shiftreduzierten Baum vor. Die folgenden Tabellen veranschaulichen die Größenordnung der erzielten Arbeitserleichterung  $b(k, m) - r(k, m)$  auch prozentual bezüglich  $b(k, m)$ .

$k$	$m$	Ersparnis	in %
2	5	26 Worte	41.3
3	5	206 Worte	56.6
5	5	2626 Worte	67.2

$k$	$m$	Ersparnis	in %
2	10	1013 Worte	49.5
3	10	58015 Worte	65.5
5	10	9385542 Worte	76.9

Trotz alledem erbt  $\mathcal{R}(G)$  das Hauptstrukturmerkmal von  $\mathcal{B}(G)$ .

#### Korollar 3.4.4

Es sei  $G = \langle x_1, x_2, \dots, x_k \rangle$ ,  $k \in \mathbb{N}$  eine endliche Gruppe. Dann gilt:

Die BFS-Traversierung des shiftreduzierten Wortbaums  $\mathcal{R}(G)$  durchläuft die Menge der darin enthaltenen Worte in längen-lexikographisch aufsteigender Reihenfolge.

**Beweis.** Da  $\mathcal{R}(G)$  aus  $\mathcal{B}(G)$  durch das schlichte Weglassen bestimmter Teilbäume hervorgeht, folgt die Behauptung direkt aus Satz 3.4.2.  $\square$

Neben den zyklischen Shifts existiert noch eine weitere Kategorie von Ballastworten.

#### Definition 3.4.5 (Kollaps eines Wortes)

Sei  $G = \langle x_1, x_2, \dots, x_k \rangle$ ,  $k \in \mathbb{N}$ , eine endliche Gruppe. Für  $1 \leq i \leq k$  sei  $n_i := \text{ord}(x_i)$ .

Ein Wort  $w \in \mathcal{W}(G)$  **kollabiert**, falls in ihm eine triviale Erzeugerpotenz  $x_i^{n_i}$  als Teilwort auftritt.

**Bemerkung:** Allgemeiner könnten wir vom Kollaps eines Wortes  $w$  sprechen, sobald *irgendein* Teilwort von  $w$  trivial ist. Im Gegensatz zu der in Definition 3.4.5 genannten Bedingung, die sich mit maximal  $|w|$  Ganzzahladditionen auswerten lässt, müssten dann jedoch alle  $\frac{1}{2}|w|(|w| + 1)$  nichtleeren Teilworte von  $w$  auf Gleichheit mit  $1_G$  geprüft werden.

In einem kollabierenden Wort  $w$  finden wir stets ein Präfix  $p$  sowie ein Suffix  $s$  mit  $|ps| < |w|$  und der Eigenschaft, dass  $w$  und  $ps$  als Gruppenelemente übereinstimmen. Laut Korollar 3.4.4 wird aber der (längen-)lexikographisch kleinste zyklische Shift von  $ps$  bereits untersucht sein, wenn die BFS-Traversierung beim Wort  $w$  ankommt, denn  $ps \sqsubset w$ .

Sofern ein Wort kollabiert, erübrigt sich deswegen jede Art von ausführlicheren Diagnosen.

### 3.4.2 Klassenvertreter mit längen-lexikographisch kleinstem Basiswort

Ohne die Ordnung der gegebenen Gruppe  $G$  und speziell den Index eines beliebigen Elementenzentralisators berechnen zu können, ist die Abbruchbedingung von Algorithmus 3.2.2 nicht evaluierbar. Für Permutationsgruppen stellen GAP und MAGMA die benötigten Funktionen zur Verfügung; eine für die Anwendung auf Matrixgruppen geeignete Schleifensteuerung soll darum im nächsten Unterabschnitt separat diskutiert werden.

Experimentelle Beobachtungen bestätigen die intuitiv einleuchtende Vermutung, dass man ein Konjugiertenklassenrepräsentantensystem  $\mathcal{S}$  erheblich schneller komplettieren kann, wenn abweichend von der reinen BFS-Strategie an gewissen Stellen des shiftreduzierten Wortbaums erst gezielt in die Tiefe statt sofort weiter in die Breite sondiert wird. Präziser ausgedrückt lohnt es sich, das natürliche „Wegenetz“ der Potenzabbildungen auf  $\mathcal{S}$  konstruktiv zu nutzen, um auf möglichst elegante Weise von einer Klasse zur nächsten zu gelangen.

Angenommen das Wort  $w$  repräsentiert eine bislang unbekannte Konjugiertenklasse von  $G$ . Für alle Exponenten  $q = 2, 3, \dots, \text{ord}(w) - 1$  sind exakt zwei Fälle zu unterscheiden:

**Fall 1:** Auch  $w^q$  repräsentiert eine bislang unbekannte Konjugiertenklasse.

**Fall 2:** Das Wort  $w^q$  liegt in einer der schon gefundenen Konjugiertenklassen. Rekursiv argumentiert ist dann außerdem jedes Wort der Gestalt  $w^{nq}$ ,  $n \geq 2$ , in  $G$  konjugiert zu einem der schon gefundenen Vertreterworte, dessen Potenzen ja längst analysiert wurden.



Dieser Gedankengang ist eng verwandt mit einer Idee von I. A. I. Suleiman, P. G. Walsh und R. A. Wilson [42], die zwei Worte  $w_1, w_2 \in \mathcal{W}(G)$  als **essenziell verschieden** bezeichnen, falls  $\langle w_1 \rangle$  und  $\langle w_2 \rangle$  keine einzige Konjugiertenklasse von  $\mathcal{W}(G)$  (aufgefasst als freie Gruppe in den Erzeugern von  $G$ ) gemeinsam anschneiden.

Schlechthin zum Nulltarif ist der durch die vorgezogene Betrachtung von Potenzworten erwirkte Geschwindigkeitsvorteil freilich nicht zu haben. So muss nun umgekehrt dafür Sorge getragen werden, dass die vorweggenommene Arbeit später nicht ein zweites Mal erledigt wird. Für ein gegebenes Wort  $w$  lässt sich anhand der Länge  $|w|$  und ihrer Teiler allerdings sehr billig entscheiden, ob  $w$  eine Potenz sein könnte, und wenn ja, von welchem seiner Präfixe.

**Algorithmus 3.4.6** (Repräsentantenworte mit längen-lexikographisch kleinster Basis)

Sei  $G$  eine Permutationsgruppe und die Teilmenge  $\{x_1, x_2, \dots, x_k\} \subseteq G$ ,  $k \in \mathbb{N}$ , ein fest gewähltes, (längen-)lexikographisch aufsteigend indiziertes Erzeugendensystem für  $G$ .

**Schritt 1**

Initialisiere die Menge der gefundenen Repräsentantenworte  $W := \{1_G\}$ .

Initialisiere die Kontrollsumme  $c = \sum_{w \in W} |(w)^G| := 1$ .

Berechne  $m := |G|$ .

**Schritt 2**

**Solange**  $c \neq m$  :

Bestimme den gemäß BFS nächsten Pfad  $\mathcal{P}$  in  $\mathcal{R}(G)$ .

Setze  $i := \text{Index des Anfangsfaktors von } w_{\mathcal{P}}$ .

**Falls**  $w_{\mathcal{P}}$  nicht kollabiert **und**  
 $w_{\mathcal{P}} \sqsubseteq s$  für alle zyklischen Shifts  $s$  von  $w_{\mathcal{P}}$  mit Anfangsfaktor  $x_i$  **und**  
 $w_{\mathcal{P}}$  keine Potenz eines seiner Präfixe ist **:**

Berechne  $d := \text{ord}(w_{\mathcal{P}})$ .

**Falls**  $w_{\mathcal{P}}$  in  $G$  zu keinem  $w \in W$  der Ordnung  $d$  konjugiert ist :

Setze  $W := W \cup \{w_{\mathcal{P}}\}$ .

Inkrementiere  $c$  um  $|(w_{\mathcal{P}})^G| = m \cdot |\mathbf{C}_G(w_{\mathcal{P}})|^{-1}$ .

Initialisiere die Menge der relevanten Exponenten  $E := \{2, 3, \dots, d-1\}$ .

Führe **Schritt 3** aus.

Springe zu **Ende**.

**Schritt 3**

**Solange**  $c \neq m$  **und**  $E \neq \emptyset$  :

Setze  $q := \min E$ .

**Falls**  $w_{\mathcal{P}}^q$  in  $G$  zu keinem  $w \in W$  der Ordnung  $\text{ord}(w_{\mathcal{P}}^q)$  konjugiert ist :

Setze  $W := W \cup \{w_{\mathcal{P}}^q\}$ .

Inkrementiere  $c$  um  $|(w_{\mathcal{P}}^q)^G| = m \cdot |\mathbf{C}_G(w_{\mathcal{P}}^q)|^{-1}$ .

Setze  $E := E \setminus \{q\}$ .

**Sonst** :

Setze  $E := E \setminus \{nq \mid n \in \mathbb{N}\}$ .

**Falls**  $c \neq m$  :

Führe **Schritt 2** aus.

**Ende**

Wir fassen die Ergebnisse dieses Unterabschnitts zusammen:

**Satz 3.4.7**

*Angewandt auf eine Permutationsgruppe  $G$  mit lexikographisch geordneter Erzeugermenge  $X$  terminiert Algorithmus 3.4.6. Die resultierende Menge  $W$  ist dann ein Vertretersystem für die Konjugiertenklassen von  $G$ , wobei alle Repräsentanten  $w \in W$  Potenz eines bezüglich  $X$  längen-lexikographisch kleinsten Basisworts sind.*

**Beweis.** Lemma 3.3.6 garantiert, dass  $\mathcal{R}(G)$  per Konstruktion ein komplettes Konjugiertenklassenvertretersystem enthält. Erwiesenermaßen unbeeinflusst von den gegenüber Algorithmus 3.2.2 ergänzten, effizienzsteigernden Schritten folgen Terminierung und Korrektheit von Algorithmus 3.4.6 deshalb analog zum Beweis von Satz 3.2.3. Die besagte Minimaleigenschaft der Worte in  $W$  ist eine unmittelbare Konsequenz aus Korollar 3.4.4 und der zusätzlich bemühten Potenz-Heuristik.  $\square$

### 3.4.3 Ein alternatives Abbruchkriterium

Sei  $G$  ab jetzt eine Matrixgruppe. Kapitulierte der Computer angesichts der Berechnung eines Elementzentralisators in  $G$ , so geht damit typischerweise auch das Scheitern der Algorithmen zum Testen zweier Elemente auf Konjugiertheit in  $G$  einher. Während das letztere Problem wenigstens approximativ gelöst werden kann, indem wir uns auf die Frage nach universeller Konjugiertheit zurückziehen, macht das erstere eine Anwendung von Algorithmus 3.4.6 auf  $G$  unmöglich, weil die Abbruchbedingung

$$\sum_{w \in W} |(w)^G| = |G|$$

praktisch nicht länger entscheidbar ist. Der verfahrensstrukturell naheliegendste Ersatz für die bisherige Schleifensteuerung dürfte eine Beschränkung der maximalen Suchtiefe im shift-reduzierten Wortbaum  $\mathcal{R}(G)$  sein. Berücksichtigt werden also bloß noch Worte, deren Länge ein zu Beginn vereinbartes Limit nicht überschreiten.

Ferner erscheint es nun sinnvoll, *sämtliche* untersuchten Worte gemäß ihrer universellen Konjugiertenklasse zu katalogisieren, denn im Anschluss an die automatisch ablaufende Prozedur sollte eine „manuelle Verfeinerung“ der Resultate möglich sein. Beispielszenarien hierfür:

- Es ist eine treue Permutationsdarstellung  $\pi$  von  $G$  bekannt, die jedoch einen zu großen Grad besitzt, als dass man Zentralisatoren oder die Antwort auf Konjugiertheitsfragen direkt in  $\pi(G)$  bestimmen könnte. Nichtsdestoweniger lassen sich zwei Elemente  $g, h \in G$  mit  $g \sim h$  dann eventuell anhand der Zykelstrukturen von  $\pi(g)$  und  $\pi(h)$  als nicht-konjugiert in  $G$  erkennen (vergleiche Lemma 3.3.3).
- Neben  $G \leq \mathrm{GL}_r(\mathbb{F}_1)$  ist noch eine weitere treue Matrixdarstellung  $\mathfrak{X} : G \rightarrow \mathrm{GL}_s(\mathbb{F}_2)$  verfügbar. Im Idealfall kann der Algorithmus dann mit  $\mathfrak{X}(G)$  wiederholt werden, was zu einer hoffentlich aussagekräftigen Kombination der jeweiligen Einzelergebnisse führt. Ansonsten vermögen vielleicht auch Spur oder Determinante auf  $\mathfrak{X}(G)$  einige universelle Konjugiertenklassen von  $G$  zu partitionieren (vergleiche Lemma 3.3.4).

- Theoretische Argumente erlauben einen Ad-hoc-Zugriff auf Strukturinformation über die Gruppe  $G$ . Anhand dieser Daten kann unter anderem etwa häufig ermittelt werden, welche Potenzen  $g^q$  eines Elements  $g \in G$  mit  $\text{ggT}(q, \text{ord}(g)) = 1$  in  $G$  niemals zu  $g$  konjugiert sein können.

Prinzipiell wäre die Potenz-Heuristik von Algorithmus 3.4.6 ebenso gut auf Matrixgruppen anwendbar. Da ohnehin alle Worte bis zu einer vorgegebenen maximalen Länge durchlaufen werden müssen, würde eine Hinzunahme der diversen Potenzen nur *mehr* Worte, diese aber keineswegs *schneller* liefern. Das folgende Verfahren verzichtet daher auf einen entsprechenden dritten Schritt.

**Algorithmus 3.4.8** (kürzeste Repräsentantenworte, Version 2)

Sei  $G$  eine endliche Matrixgruppe und die Teilmenge  $\{x_1, x_2, \dots, x_k\} \subseteq G$ ,  $k \in \mathbb{N}$ , ein fest gewähltes, (längen-)lexikographisch aufsteigend indiziertes Erzeugendensystem für  $G$ . Darüber hinaus bezeichne  $m \in \mathbb{N}_0$  die maximale Länge der zu betrachtenden Worte.

**Schritt 1**

Initialisiere die Menge der gefundenen universellen Vertreterworte  $W := \{1_G\}$ .  
Initialisiere den aktuellen Pfad  $\mathcal{P} := \mathcal{P}_{x_1}$  in  $\mathcal{R}(G)$  und die aktuelle Wortlänge  $\ell := 1$ .

**Schritt 2**

**Solange**  $\ell \leq m$  :

Setze  $i := \text{Index des Anfangsfaktors von } w_{\mathcal{P}}$ .

**Falls**  $w_{\mathcal{P}}$  nicht kollabiert

**und**

$w_{\mathcal{P}} \sqsubseteq s$  für alle zyklischen Shifts  $s$  von  $w_{\mathcal{P}}$  mit Anfangsfaktor  $x_i$  :

Berechne  $d := \text{ord}(w_{\mathcal{P}})$ .

**Falls**  $d \neq 1$  : /\* Ansonsten gilt nämlich sicher  $(w_{\mathcal{P}})_G = (w_{\mathcal{P}})^G$ . \*/

Suche das  $w \in W$  mit  $\text{RKF}(w_{\mathcal{P}}) = \text{RKF}(w)$ .

**Falls** kein solches Vertreterwort existiert :

Setze  $W := W \cup \{w_{\mathcal{P}}\}$ .

Initialisiere die Wortliste  $L(w_{\mathcal{P}}) := [ ]$ .

**Sonst** :

Setze  $L(w) := L(w) \cup [w_{\mathcal{P}}]$ .

Bestimme den gemäß BFS nächsten Pfad  $\mathcal{P}$  in  $\mathcal{R}(G)$ .

Setze  $\ell := |w_{\mathcal{P}}|$ .

**Ende**

Trivialerweise terminiert Algorithmus 3.4.8. Aus Lemma 3.3.4(c) und Korollar 3.4.4 ergibt sich mithin

**Satz 3.4.9**

Angesetzt auf eine endliche Matrixgruppe  $G$  mit lexikographisch geordneter Erzeugermenge  $X$  und ein Wortlängenlimit  $m \in \mathbb{N}_0$  produziert Algorithmus 3.4.8 ein Vertretersystem  $W$  für die universellen Konjugiertenklassen von  $G$ , die bezüglich  $X$  Worte einer Länge  $\leq m$  enthalten. Für jedes Repräsentantenwort  $w \in W$  ist dabei  $[w] \cup L(w)$  eine längen-lexikographisch aufsteigend sortierte Wortliste, die bezüglich  $X$  und modulo zyklischer Shifts alle zu  $w$  universell konjugierten Worte einer Länge  $\leq m$  aufführt.

### 3.5 Implementierung und qualitatives Laufzeitverhalten

Algorithmus 3.4.6 wurde sowohl für GAP [13] als auch für MAGMA [2] implementiert. Aufgrund der relativ spartanischen Matrizen-Funktionalität unter GAP existiert eine lauffähige Umsetzung von Algorithmus 3.4.8 derzeit lediglich für MAGMA.

Der gesamte zugehörige Programmcode ist gemäß den Richtlinien der GNU General Public License<sup>3</sup> frei verfügbar und befindet sich im Format eines (unkomprimierten) **tar**-Archivs auf der beiliegenden Diskette<sup>4</sup>. Von dort kann er somit auf jedem UNIX- oder Linux-Rechner durch Eingabe des Extraktionsbefehls

```
tar xvf /dev/fd0
```

innen Sekunden installiert werden.

Nach dem Einlesen der Datei `ccs.gap` in eine GAP-Sitzung bzw. der Datei `ccs.magma` in eine MAGMA-Sitzung kennt das jeweilige System dann sämtliche der im Folgenden dokumentierten Datenstrukturen und Funktionen.

#### 3.5.1 Worte in Erzeugern, Konjugiertenklassensysteme und Wortlisten

Sei  $G$  eine endliche Gruppe und die Teilmenge  $\{x_1, x_2, \dots, x_k\} \subseteq G$ ,  $k \in \mathbb{N}$ , ein fest gewähltes, Erzeugendensystem für  $G$ .

**Worte**  $w \in \mathcal{W}(G)$  wurden als *GAP-Listen* bzw. *MAGMA-Sequenzen* von natürlichen Zahlen implementiert, wobei der  $i$ -te Eintrag einer derartigen Liste bzw. Sequenz gerade den Index des  $i$ -ten Faktors von  $w$  wiedergibt, zum Beispiel:

$$x_2 x_4 x_7^2 x_3 x_5^3 x_4 \longleftrightarrow [2, 4, 7, 7, 3, 5, 5, 5, 4]$$

Dass GAP und MAGMA auf der Menge solcher Sequenzen bereits von Haus aus die durch die kanonische Ordnung auf  $\mathbb{N}$  induzierte lexikographische Ordnung verwenden, ist ein Umstand, der sich insbesondere beim paarweisen Vergleich der zyklischen Shifts eines Wortes  $w \in \mathcal{W}(G)$  bezüglich  $\sqsubseteq$  günstig auf die benötigte Rechenzeit auswirkt.

Zur Verwaltung der mannigfaltigen Information, die über das **System der Konjugiertenklassen** von  $G$  Schritt für Schritt in Erfahrung gebracht wird, eignet sich ein Verbundobjekt oder *Record*. Während GAP seinen Benutzern nahezu alle Freiheiten lässt, was die Definition sowie die dynamische Erweiterung eines Records um neue Komponenten angeht, muss unter MAGMA für jeden Record eine statische Syntax, das so genannte *Record-Format*, erklärt werden.

Ein Verbundobjekt `ccs` vom Typ `ConjugacyClassSystem` besteht aus den Komponenten

**assocGroup :**

die Gruppe  $G$ , deren Konjugiertenklassensystem durch `ccs` dargestellt wird;

**nClasses :**

die Anzahl der Konjugiertenklassen von  $G$ ;

---

<sup>3</sup>Siehe `gnupl.txt` auf der beiliegenden Diskette oder <http://www.gnu.org/copyleft/gpl.html>.

<sup>4</sup>Diskette fehlt? Eine E-Mail an [kratzer@exp-math.uni-essen.de](mailto:kratzer@exp-math.uni-essen.de) genügt! Unter ebendieser Adresse sind übrigens auch Kommentare, Anregungen und Kritik jederzeit willkommen.

**repOfClass :**

das eigentliche Repräsentantensystem für die Konjugiertenklassen von  $G$ ; eine Liste von Vertreterworten  $w \in \mathcal{W}(G)$ , die so sortiert ist, dass ...

**ordOfRep**

..., die Sequenz der Repräsentantenordnungen, eine monoton steigende Liste natürlicher Zahlen ist, deren  $i$ -ter Eintrag gerade der Ordnung von  $ccs.repOfClass[i]$  entspricht,

**lenOfClass**

..., die Sequenz der Klassenlängen, eine sektionsweise *steigende* Liste natürlicher Zahlen ist, deren  $i$ -ter Eintrag gerade der Länge von  $(ccs.repOfClass[i])^G$  entspricht, und

**ordOfCent**

..., die Sequenz der Zentralisatorordnungen, eine sektionsweise *fallende* Liste natürlicher Zahlen ist, deren  $i$ -ter Eintrag gerade der Ordnung von  $C_G(ccs.repOfClass[i])$  entspricht.

**distOfOrders :**

die Ordnungsverteilung von  $G$ ; eine Sequenz von bezüglich ihrer ersten Komponente streng monoton steigend sortierten Tripeln  $[ord, num, lst]$ . Diese besagen, dass die Gruppe  $G$  exakt  $num$  Konjugiertenklassen mit Elementen der Ordnung  $ord$  besitzt, von denen  $(ccs.repOfClass[lst])^G$  die reihenfolgemäßig letzte in  $ccs$  ist.

**instPowMaps :**

eine aktuelle Liste der Primzahlexponenten  $p$ , zu denen die jeweilige Potenzabbildung in  $ccs$  installiert wurde;

**pPowermap :**

die Sequenz der aktuell in  $ccs$  installierten Potenzabbildungen, wobei die Position des Exponenten  $p$  in  $ccs.instPowMaps$  gerade mit der Position der  $p$ -Potenzabbildung in  $ccs.pPowermap$  übereinstimmt.

Jede  $p$ -Potenzabbildung ist wiederum als Liste der Länge  $ccs.nClasses$  implementiert, deren  $i$ -ter Eintrag genau dann gleich  $j$  ist, wenn gilt:

$$(ccs.repOfClass[i]^p)^G = (ccs.repOfClass[j])^G.$$

Die im Rahmen von Algorithmus 3.4.8 auftretenden **Wortlisten**  $L(w)$ ,  $w \in \mathcal{W}(G)$ , werden zur Laufzeit üblicherweise sehr schnell sehr groß. Es erscheint deswegen angebracht, sie als ASCII-Textdateien zu realisieren, zumal ihr Inhalt in der Regel sowieso „manuell“ nachbearbeitet werden muss.

### 3.5.2 Die Funktionen der ccs-Bibliothek

Mit Ausnahme der letzten existiert jede der nachfolgend dokumentierten Funktionen und Prozeduren sowohl in  $ccs.gap$  als auch in  $ccs.mag$ .

**EratosthenesSift(  $M, n$  ) :**

streicht (destruktiv) alle Vielfachen der Zahl  $n$  aus der Menge  $M$ .

**InstallPrimePowermap**( *ccs*, *p* ) :

konstruiert und installiert die zum Primzahlexponenten  $p$  gehörige Potenzabbildung auf dem Konjugiertenklassensystem *ccs*.

**IsCollapsingWord**( *w*, *gen\_orders* ) :

liefert **true** genau dann, wenn das Wort  $w$  kollabiert; sonst lautet der Rückgabewert **false**. Der Liste *gen\_orders* muss die Funktion dazu an  $i$ -ter Stelle die Ordnung des Gruppenerzeugers  $x_i$  entnehmen können.

**IsLessThan4ConjugacyClasses**( *cc*<sub>1</sub>, *cc*<sub>2</sub> ) :

eine totale Ordnungsrelation auf der Menge der Konjugiertenklassen einer Gruppe; die Klasse *cc*<sub>1</sub> heißt in diesem Zusammenhang **kleiner als** die Klasse *cc*<sub>2</sub>, falls

- die Ordnung der Elemente von *cc*<sub>1</sub> kleiner ist als die der Elemente von *cc*<sub>2</sub>, *oder*
- die Elemente beider Klassen dieselbe Ordnung haben, aber die Länge von *cc*<sub>1</sub> kleiner ist als die Länge von *cc*<sub>2</sub>, *oder*
- die Elemente beider Klassen dieselbe Ordnung und beide Klassen dieselbe Länge haben, aber das Basiswort des Repräsentanten von *cc*<sub>1</sub> längen-lexikographisch kleiner ist als das Basiswort des Repräsentanten von *cc*<sub>2</sub>, *oder*
- beide Klassen Elemente derselben Ordnung, die gleiche Länge und Repräsentanten mit demselben Basiswort haben, aber der Exponent dieses Worts beim Repräsentanten von *cc*<sub>1</sub> kleiner ist als beim Repräsentanten von *cc*<sub>2</sub>.

**IsLexLowestCyclicShift**( *w* ) :

liefert **true** genau dann, wenn kein zyklischer Shift des Wortes  $w$  (längen-) lexikographisch kleiner ist als  $w$  selbst; andernfalls lautet der Rückgabewert **false**.

**IsPowerWord**( *w*, *n* ) :

liefert **true** genau dann, wenn das Wort  $w$  eine Konkatenation aus  $n$  gleichen Teilworten ist; andernfalls lautet der Rückgabewert **false**.

**LexLowestBaseConjugacyClassRepresentatives**( *G* ) :

berechnet ein Repräsentantensystem für die Konjugiertenklassen der Permutationsgruppe  $G$  derart, dass jeder Repräsentant Potenz eines bezüglich der Erzeugermenge von  $G$  längen-lexikographisch kleinsten Wortes ist.

Als Rückgabeobjekt wird ein Record (vom Format **ConjugacyClassSystem**) generiert, dessen Potenzabbildungs-Komponenten zunächst undefiniert bleiben.

Über globale Variablen (in GAP) bzw. Funktionsparameter (in MAGMA) lässt sich

- bei Bedarf steuern, in welchem Umfang Zwischenstände der Rechnung ausgegeben werden sollen;
- eine unterbrochene Rechnung ab dem zuletzt durchsuchten Erzeuger-Wortbaum neu aufsetzen.

**MakeStepBFS**( *w*, *min*, *max* ) :

inkrementiert das Wort  $w$  gemäß einer BFS-Traversierung des vollständigen Wortbaums über den Erzeugern  $min$ ,  $min+1$ , ...,  $max$ .

**PowerClass( *ccs*, *i*, *q* ) :**

ermittelt den Index derjenigen Konjugiertenklasse im System *ccs*, welche von der *q*-ten Potenz des Wortes *ccs.repOfClass[i]* repräsentiert wird.

**SeqInt2GrpElt( *G*, *w* ) :**

liefert das als Element von *G* ausmultiplizierte Wort *w*. Die leere Sequenz wird hier als leeres Wort interpretiert und bewirkt infolge dessen die Rückgabe von  $1_G$ .

Jeder nicht-positive Eintrag von *w* führt ebenso zu einer Fehlermeldung wie ein Eintrag, der größer als die Anzahl der Erzeuger von *G* ist.

**Translate2LaTeX( *ccs*, *grp\_id*, *gen\_ids*, *file* ) :**

erzeugt aus der im Konjugiertenklassensystem *ccs* enthaltenen Information eine entsprechende L<sup>A</sup>T<sub>E</sub>X<sub>2 $\epsilon$</sub> -Quelldatei *file*. Welche Bezeichner dabei für die zugrunde liegende Gruppe bzw. deren Erzeuger verwendet werden sollen, kann der Aufrufer durch die Wahl der Zeichenkette *grp\_id* bzw. der Liste *gen\_ids* von Zeichenketten selbst bestimmen.

**UniversalConjugacyClassRepresentatives( *G*, *max*, *gen\_ids* ) :**

produziert ein Repräsentantensystem für diejenigen universellen Konjugiertenklassen der Matrixgruppe *G*, welche bezüglich der Erzeugermenge von *G* Worte einer Länge kleiner oder gleich *max* enthalten.

Beginnend mit dem jeweiligen Repräsentantenwort  $w \in \mathcal{W}(G)$  wird in einem Unterverzeichnis namens **UniConClsd** mit  $d = \text{ord}(w)$  eine längen-lexikographisch aufsteigend sortierte Wortliste abgelegt, die bezüglich der Erzeugermenge von *G* und modulo zyklischer Shifts alle zu *w* universell konjugierten Worte einer Länge kleiner oder gleich *max* aufführt. Welche Bezeichner dabei für die Erzeuger von *G* verwendet werden sollen, kann der Aufrufer durch die Wahl der Liste *gen\_ids* von Zeichenketten selbst bestimmen.

### 3.5.3 Bemerkungen zur Komplexität

Grundsätzlich kostet die BFS-Traversierung eines *k*-nären Baumes von seiner Wurzel bis zur Tiefe *d* exponentiell viele, nämlich  $\mathcal{O}(k^d)$  Rechenschritte. Diese Abschätzung ist jedoch zumindest für Algorithmus 3.4.6 bei weitem zu pessimistisch.

Zum einen wird gar kein vollständiger *k*-närer Baum durchlaufen, sondern nur eine dem gegenüber erheblich ausgedünnte Struktur. Zum anderen beschleunigt die Potenz-Heuristik das Verfahren ganz entscheidend, indem es die reine BFS-Strategie gezielt verfremdet. Verglichen mit einem Test zweier universell konjugierter Elemente auf Konjugiertheit in der betreffenden Gruppe *G* ist ein Traversierungsschritt in  $\mathcal{R}(G)$  vom Zeitaufwand her nahezu vernachlässigbar. Weil umgekehrt ein solcher Test insgesamt relativ selten — in Algorithmus 3.4.8 sogar niemals — durchgeführt werden muss, erweist sich der Backtracking-Ansatz trotz seiner exponentiellen Veranlagung als durchaus praktikabel.

Die reale mittlere Komplexität der beiden Verfahren quantitativ zu analysieren ist äußerst schwierig, hängt sie doch in hohem Maße von der statistischen Verteilung der gesuchten Konjugiertenklassenrepräsentanten in der Menge  $\mathcal{W}(G)$  ab. Diese Verteilung wiederum variiert mit der Wahl des Erzeugendensystems für *G*, die letztendlich der Benutzer trifft und deshalb einen absolut unwägbaren Faktor darstellt:

Während die symmetrische Gruppe  $G = S_4$  von der Menge der in Beispiel 3.1.2 angegebenen Konjugiertenklassenrepräsentanten erzeugt wird, was für Algorithmus 3.4.6 lineare(!) Laufzeit bedeutet, lässt sich dieselbe Gruppe genauso gut mit zwei in  $G$  konjugierten Permutationen, etwa  $x = (1, 2, 3, 4)$  und  $y = (1, 3, 2, 4)$  erzeugen. Den Repräsentanten für die Involutionenklasse  $2_2 = ((1, 2))^G$  finden wir dann allerdings erst in Tiefe 3 des shiftreduzierten Wortbaumes  $\mathcal{R}(G)$ .

Intuitiv würde man sicherlich erwarten, dass eine größere Erzeugermenge automatisch zu kürzeren Vertreterworten führt. Versuche in diese Richtung haben aber gezeigt, dass selbst dieser Zusammenhang im Allgemeinen ein Trugschluss ist. Viele wie im oben „ungeschickt“ gewählte Erzeuger tragen höchstens dazu bei, die Rechenzeit zu verlängern.

Als Faustregel bewährt hat sich hingegen die Taktik, so viele Erzeuger wie nötig von so hoher Ordnung wie möglich zu wählen.

### 3.6 Berechnung der irreduziblen $\mathbb{C}$ -Charaktere

Wie angekündigt schließt dieses Kapitel mit einem Exkurs über die computeralgebraischen Methoden zur Bestimmung der irreduziblen  $\mathbb{C}$ -Charaktere einer endlichen Gruppe  $G$ . Das probate, von seinen Voraussetzungen her generell anwendbare und daher Standardlösungsverfahren ist der Algorithmus von J. D. Dixon [12] und G. J. A. Schneider [38]. Im Wesentlichen operiert er auf dem Zentrum der Gruppenalgebra  $\mathbb{C}G$  und gewinnt die Menge  $\text{Irr}_{\mathbb{C}}(G)$  anhand der Multiplikationskonstanten von  $\mathbf{Z}(\mathbb{C}G)$  bezüglich der Basis, welche aus den Konjugiertenklassensummen

$$\bar{K}(x) = \sum_{y \in (x)^G} y \in \mathbb{C}G, \quad x \in G,$$

besteht. Die präzise Vorgehensweise ist darauf getrimmt, tunlichst wenige Multiplikationskonstanten explizit ausrechnen zu müssen, denn exakt diese Aufgabe nimmt den Löwenanteil der benötigten Rechenzeit und für genügend „große“ Gruppen schnell mehr Speicherplatz als verfügbar in Anspruch.

Außer dem Dixon-Schneider-Algorithmus, der  $\text{Irr}_{\mathbb{C}}(G)$  quasi unmittelbar aus der Gruppe  $G$ , will heißen aus der Interaktion ihrer Elemente ableitet, gibt es freilich noch ein breites Spektrum an rein charaktertheoretischen Methoden zur Ermittlung der irreduziblen  $\mathbb{C}$ -Charaktere von  $G$ . Einziges Manko dieser Werkzeuge ist ihr gemeinsames Funktionsprinzip: Aus *schon bekannten* (am besten irreduziblen) Charakteren können sie rasant neue und mit etwas Glück irreduzible konstruieren. Doch woher soll die Vorgabe kommen?

#### □ Zerlegung transitiver Permutationscharaktere

Sei  $M$  eine Untergruppe in  $G$  vom Index  $n := |G : M|$ , und sei die Menge  $T = \{g_1, g_2, \dots, g_n\}$  eine Rechtstransversale von  $M$  in  $G$ , wobei ohne Einschränkung  $g_1 = 1_G$  gelte. Die kanonische Operation von  $G$  auf  $\Omega := \{Mg_r \mid g_r \in T\}$  induziert die Permutationsdarstellung  $(\mathbb{1}_M)^{\uparrow G}$ ; der zugehörige Permutationsmodul über  $\mathbb{C}$  sei im Folgenden mit  $P$  bezeichnet.

In [33] beschreiben G. O. Michler und M. Weller eine Methode zur Zerlegung des von  $(\mathbb{1}_M)^{\uparrow G}$  erzeugten Permutationscharakters  $\pi$  in irreduzible Konstituenten. Betrachtet wird dazu eine



Partitionierung der Gruppe  $G$  in  $M$ - $M$ -Doppelnebenklassen, etwa

$$G = \bigcup_{k=1}^d Mx_kM \quad \text{mit} \quad x_1 = 1_G .$$

Für jede Doppelnebenklasse  $Mx_kM$  erhält man eine *Intersection-Matrix*  $D_k \in \text{Mat}_d(\mathbb{C})$ , die sich aus ganzzahligen, nicht-negativen Einträgen zusammensetzt.

Die Menge  $\{D_k \mid 1 \leq k \leq d\}$  ist linear unabhängig über jedem Körper und bildet die Basis einer zum Hecke-Ring  $\mathcal{H} = \text{End}_{\mathbb{C}G}(P)$  isomorphen Subalgebra  $\mathcal{I} \leq \text{Mat}_d(\mathbb{C})$ , der so genannten *Intersection-Algebra*. Zwischen den irreduziblen Konstituenten  $\chi$  von  $\pi$  und den zentralen primitiven Idempotenten

$$e = \sum_{k=1}^d a_k D_k \tag{C}$$

von  $\mathcal{I}$  existiert demnach eine Bijektion  $\chi \mapsto e_\chi$  bzw.  $e \mapsto \chi_e$ .

Michler und Weller geben in dieser Situation ein effizientes Verfahren zur Berechnung der in der Linearkombination (C) auftretenden Koeffizienten  $a_k \in \mathbb{C}$  an und beweisen, dass der zu  $e$  korrespondierende Konstituent  $\chi_e$  von  $\pi$  auf einer Konjugiertenklasse  $(x)^G$  gerade den Wert

$$\chi_e(x) = [\chi_e, \pi]_G \cdot \sum_{k=1}^d \overline{a_k} \left| \{Mg_r \in \Omega \mid Mg_r x g_r^{-1} \subseteq Mx_kM\} \right| \tag{D}$$

annimmt, wobei sich die Multiplizität  $[\chi_e, \pi]_G$  ebenso wie der Grad  $\chi_e(1_G)$  direkt aus Eigenschaften des Idempotents  $e$  erschließen lassen. Dieses Resultat verallgemeinert in gewissem Sinne den Algorithmus von Dixon und Schneider, welcher letztendlich die Konstituenten der regulären Darstellung von  $G$  bestimmt<sup>5</sup>.

Der in Gleichung (D) von Summand zu Summand variierende Mächtigkeitsfaktor entstammt ursprünglich einer Klassensummenformel von H. W. Gollan und T. W. Ostermann [14].

**Definition 3.6.1 (Gollan-Ostermann-Vektor)**

Sei  $G$  eine endliche Gruppe,  $M \leq G$ ,  $n := |G : M|$ , und sei  $\Omega = \{Mg_1, Mg_2, \dots, Mg_n\}$  die Menge der Rechtsnebenklassen von  $M$  in  $G$ . Ferner sei  $G = \bigcup_{k=1}^d Mx_kM$  eine Partitionierung von  $G$  in  $M$ - $M$ -Doppelnebenklassen.

Für jedes Element  $x \in G$  ist dann der Vektor  $\text{GO}_M(x) := (m_1, m_2, \dots, m_d) \in \mathbb{N}_0^d$ , worin

$$m_k := \left| \{Mg_r \in \Omega \mid Mg_r x g_r^{-1} \subseteq Mx_kM\} \right|, \quad 1 \leq k \leq d,$$

offensichtlich unabhängig von der speziellen Vertreterwahl  $g_r$ ,  $1 \leq r \leq n$ , bzw.  $x_k$ ,  $1 \leq k \leq d$ , und heißt der **Gollan-Ostermann-Vektor von  $x$  bezüglich  $M$** .

Fünf Maßnahmen versetzen uns in die Lage,  $\text{GO}_M(x)$  mit minimalem Aufwand ausrechnen zu können, falls  $G$  auf  $\Omega$  treu operiert (ohne Einschränkung gelte wieder  $g_1 = x_1 = 1_G$ ):

1. Identifizierung der Gruppe  $G$  mit ihrem Bild unter der Permutationsdarstellung  $(\mathbb{1}_M)^\uparrow^G$ ; dadurch wird aus einer Rechtsnebenklasse  $Mg_r$  die Ziffer  $r$ , und aus den Doppelnebenklassen  $Mx_kM$  werden die  $M$ -Orbits  $(1^{x_k})^M$  auf  $\Omega = \{1, 2, \dots, n\}$ .

---

<sup>5</sup>Vergleiche Korollar 5.1 in [33].

2. Simultane Bestimmung aller Komponenten  $m_k$ ,  $1 \leq k \leq d$ , innerhalb eines einzigen Durchlaufs der Ziffernmenge  $\Omega$ ; hierzu wird  $\text{GO}_M(x)$  mit  $(0, 0, \dots, 0) \in \mathbb{N}_0^d$  initialisiert und genau dann an Position  $k$  inkrementiert, wenn  $r^{xg_r^{-1}} \in (1^{x_k})^M$ .
3. (GOLLAN, OSTERMANN) Beachtung der Zykelstruktur von  $x$ ; aus  $r^{xg_r^{-1}} \in (1^{x_k})^M$  folgt sofort  $(r^{x^q})^{x(g_r x^q)^{-1}} \in (1^{x_k})^M$ , das heißt mit einer Ziffer  $r \in \Omega$  werden zugleich sämtliche Ziffern  $s \in (r)^{\langle x \rangle}$  von  $xg_s^{-1}$  in den  $M$ -Orbit  $(1^{x_k})^M$  geworfen.
4. Pragmatische Nutzung der Information im Schreier-Vektor zum Orbit  $\Omega = (1)^G$ ; statt das Repräsentanteninverse  $g_r^{-1}$  als Element von  $G$  aufzubauen, reicht es, den Weg von Ziffer 1 zu Ziffer  $r$  rückwärts auf das Bild  $r^x$  anzuwenden.
5. Einmalige Vorabberechnung der Partitionierung von  $\Omega$  in  $M$ -Orbits; hierzu wird ein Feld der Länge  $n$  mit Nulleinträgen initialisiert und erhält an Position  $p$  genau dann den Eintrag  $k$ , wenn beim Durchlauf des  $M$ -Orbits  $(1^{x_k})$  die Ziffer  $p$  gefunden wird. Eine Frage nach dem  $M$ -Orbit, der die Ziffer  $r^{xg_r^{-1}}$  enthält, kann somit einfach durch Auslesen des entsprechenden Feldeintrags beantwortet werden.

Jeder dieser „Tricks“ ist mutatis mutandis auch auf den Fall anwendbar, dass  $\text{GO}_M(x)$  für ein gesamtes System  $\mathcal{S}$  von Konjugiertenklassenrepräsentanten  $x$  der Gruppe  $G$  ermittelt werden soll. Insbesondere müssen wir die Menge  $\Omega$  nicht mehr als einmal durchlaufen: An die Stelle des einzelnen Bildes  $r^{xg_r^{-1}}$  tritt schlicht ein Feld von Bildern  $r^{xg_r^{-1}}$ ,  $x \in \mathcal{S}$ .

#### □ Ein Präprozessor für den Dixon-Schneider-Algorithmus

Sei  $G$  ab jetzt wieder eine beliebige endliche Gruppe. Sobald eine treue und transitive Permutationsdarstellung  $\varphi : G \rightarrow S_n$  bekannt ist, lohnt es sich vorwiegend für großen Grad  $n$ , dem Standardverfahren zur Charaktertafelberechnung die Arbeit wie folgt zu erleichtern:

##### **Schritt 1**

Identifiziere  $G$  mit  $\varphi(G)$ .

Bestimme den Stabilisator  $M := \text{Stab}_G(1)$ .

Bestimme gemäß Michler und Weller [33] die Menge  $\mathcal{K}$  aller irreduziblen Konstituenten des von  $(\mathbb{1}_M)^{\uparrow G}$  erzeugten Permutationscharakters  $\pi : G \rightarrow \mathbb{C}$ .

##### **Schritt 2**

Initialisiere die Menge der linken Tensorfaktoren  $\mathcal{L} := \mathcal{K}$ .

Initialisiere die Menge der rechten Tensorfaktoren  $\mathcal{R} := \mathcal{K}$ .

Setze  $k_{\text{alt}} := 0$  und  $k_{\text{neu}} := |\mathcal{K}|$ .

**Solange**  $k_{\text{alt}} < k_{\text{neu}}$  :

Setze  $k_{\text{alt}} := k_{\text{neu}}$ .

Initialisiere die Menge der neu gefundenen irreduziblen Charaktere  $\mathcal{N} := \emptyset$ .

Bilde die Menge der elementweisen Tensorprodukte  $\mathcal{T} := \mathcal{L} \otimes \mathcal{R}$ .

Reduziere die Elemente von  $\mathcal{T}$  um eventuelle Konstituenten aus  $\mathcal{K}$ .

Wende den LLL-Algorithmus [28] ([39]/[13]) auf das  $\mathbb{Z}$ -Gitter  $\Gamma := (\langle \mathcal{T} \rangle, [\cdot, \cdot]_G)$  an;

füge die dabei gefundenen irreduziblen Charaktere der Menge  $\mathcal{N}$  hinzu und

baue eine maximale linear unabhängige Teilmenge  $\mathcal{L}$  des LLL-Residuums von  $\Gamma$  auf.

Setze  $\mathcal{K} := \mathcal{K} \cup \mathcal{N}$  und  $k_{\text{neu}} := |\mathcal{K}| + |\mathcal{L}|$ .

Setze  $\mathcal{L} := \mathcal{L} \cup \mathcal{N}$  und  $\mathcal{R} := \mathcal{R} \cup \mathcal{N}$ .

Während für **Schritt 1** lediglich ein Repräsentantensystem  $\mathcal{S}$  der Konjugiertenklassen von  $G$  notwendig ist, müssen in **Schritt 2** bereits die Längen all dieser Klassen bekannt sein, da hier innere Produkte von Charakteren berechnet werden.

Um den nächsten Schritt ausführen zu können, bedarf es schließlich sämtlicher Potenzabbildungen auf  $\mathcal{S}$  zu Primzahlexponenten  $q \leq \max\{\text{ord}(g) \mid g \in G\}$ :

**Schritt 3**

Bestimme die Menge

$$\mathcal{A} := \{\chi^{[\text{sgn}]} \mid \chi \in \mathcal{K}, \text{sgn} \in \text{Irr}_{\mathbb{C}}(S_p), p \text{ ein Primteiler von } |G|\}$$

aller  $p$ -ten *antisymmetrischen Anteile* [39]/[13] der Elemente von  $\mathcal{K}$ .

Reduziere die Elemente von  $\mathcal{A}$  um eventuelle Konstituenten aus  $\mathcal{K}$ .

Setze  $\mathcal{L} := \mathcal{L} \cup \mathcal{A}$ .

Bestimme die Menge

$$\mathcal{C} := \{\vartheta \uparrow^G \mid \vartheta \in \text{Irr}_{\mathbb{C}}(\langle x \rangle), x \in \mathcal{S}\}$$

aller aus zyklischen Untergruppen von  $G$  hochinduzierten Charaktere [39]/[13].

Reduziere die Elemente von  $\mathcal{C}$  um eventuelle Konstituenten aus  $\mathcal{K}$ .

Setze  $\mathcal{L} := \mathcal{L} \cup \mathcal{C}$ .

**Schritt 4**

Wende den LLL-Algorithmus [28] ([39]/[13]) auf das  $\mathbb{Z}$ -Gitter  $\Lambda := (\langle \mathcal{L} \rangle, \llbracket \cdot, \cdot \rrbracket_G)$  an und füge die dabei gefundenen irreduziblen Charaktere der Menge  $\mathcal{K}$  hinzu.

**Schritt 5**

**Falls** das LLL-Residuum von  $\Lambda$  nicht trivial ist :

Versuche gemäß W. Plesken [36] ([39]/[13]) *orthogonale Einbettungen* dieses Residuums in ein  $\mathbb{Z}$ -Gitter der Dimension  $|\mathcal{S}| - |\mathcal{K}|$  zu konstruieren und

füge die dabei gefundenen irreduziblen Charaktere der Menge  $\mathcal{K}$  hinzu.

**Ende**

Gilt nach Abschluss dieser Prozedur  $\mathcal{K} \neq \text{Irr}_{\mathbb{C}}(G)$ , so ist der Dixon-Schneider-Algorithmus gefordert, die Charaktertafel von  $G$  zu komplettieren. Weil sich nun viele der dafür benötigten Multiplikationskonstanten leicht aus den Elementen von  $\mathcal{K}$  ableiten lassen, ist diese Vervollständigung in der Regel auch dann noch möglich, wenn eine Berechnung der gesamten Tafel mangels Hardwareressourcen scheitert.

Dass die optimale Endsituation  $\mathcal{K} = \text{Irr}_{\mathbb{C}}(G)$  keineswegs nur für praktisch uninteressante Triviale Fälle erzielt wird, zeigt

**Beispiel 3.6.2** *Eine konkrete Charaktertafel für die größte Janko-Gruppe  $J_4$ .*

Sei  $G = \langle x, y, c \rangle \cong J_4$ , wobei  $x, y$  und  $c$  die von G. O. Michler und M. Weller [32] verwendeten Erzeugermatrizen aus  $\text{GL}_{112}(2)$  respektive ihre isomorphen Bilder in  $\text{GL}_{1333}(11)$  bezeichnen. Die folgende Tabelle gibt ein Vertretersystem für die Konjugiertenklassen von  $G$  wieder, welches mit Hilfe von Algorithmus 3.4.8 und geeigneten Nachuntersuchungen ermittelt wurde:

Ordnung	Repräsentant	Spur GF(11)
1	$1_G$	2
2	$y^5$	0
	$(x^2y^2)^2$	9
3	$(x^3c)^2$	10
4	$x^2y^2$	5
	$x^3y^2cy$	8
	$x^3y^2c^3yc^2$	0
5	$y^2$	3
6	$x^3c$	2
	$x^7$	1
	$x^3y^2xy$	9
7	$xy^4$	6
	$(x^3y)^2$	4
8	$xy cyc$	1
	$(yc)^3$	8
	$y^2c^2yc^2$	1
10	$y$	10
	$yc^2$	3
11	$ycyc^2$	2
	$(xcy)^2$	2
12	$x^2c$	2
	$y^3c$	0
	$x^3y^2$	9
14	$x^3$	5
	$x^3y$	4
	$x^3yc$	7
	$y^2cyc^2$	6
15	$y^2c$	0
16	$xc^2$	10
20†	$xcyc^3$	10
	$(xcyc^3)^3$	10

Ordnung	Repräsentant	Spur GF(11)
21	$x^2$	4
	$y^2c^2$	6
22	$xcy$	9
	$xc^4$	0
23	$c$	10
24†	$yc$	0
	$(yc)^{-1}$	0
28	$xc^3$	5
	$x^3c^2$	7
29	$x^2cxy$	10
30	$yc^3$	0
31	$xy^2$	0
	$xcyc$	0
	$x^2cxc^2$	0
33	$(xy)^2$	10
	$xy^2c^2$	10
35	$x^2cxyz$	4
	$x^2c^2x^2c$	6
37†	$x^2y^3$	1
	$(x^2y^3)^2$	1
	$(x^2y^3)^3$	1
40†	$xyz^2$	1
	$(xyz^2)^3$	1
42	$x$	7
	$x^5$	5
43	$x^2c^2$	0
	$x^2yxy$	0
	$xyxy^2$	0
44	$x^2yc$	0
66	$xy$	1
	$x^3cx^2c$	1

Zu jeder in der Gruppe  $J_4$  vorkommenden Elementordnung  $n$  hat Z. Janko [21] auf theoretischem Weg sowohl die Anzahl als auch die jeweilige Länge der Konjugiertenklassen mit Elementen der Ordnung  $n$  bestimmt. Auf der Basis dieser Vorarbeit konnte definitiv entschieden werden, welche durch Algorithmus 3.4.8 identifizierten universellen Konjugiertenklassen von  $G$  sogar Konjugiertenklassen im üblichen Sinne sind.

Bis auf die einer mit  $\dagger$  versehenen Ordnung lassen sich alle Konjugiertenklassenrepräsentanten an ihrer rationalen kanonischen Form in  $\mathrm{GL}_{112}(2)$  bzw. an ihrer Spur in  $\mathrm{GL}_{1333}(11)$  (für Vertreter einer durch 7 teilbaren Ordnung) erkennen.

Für die Elemente  $g \in G$  der Ordnung 20, 24, 37 oder 40 liefert eine theoretische Analyse der Faktorgruppe

$$A(\langle w \rangle) := \mathbf{N}_{J_4}(\langle g \rangle) / \mathbf{C}_{J_4}(\langle g \rangle)$$

die  $A(\langle g \rangle)$ -Orbits auf  $\langle g \rangle$ , an denen sich ablesen lässt, welche Potenzen von  $g$  in  $G$  nicht zu  $g$  konjugiert sein können. Das notwendige Wissen über die Untergruppenstruktur einer Gruppe vom Typ  $J_4$  ist zum Teil der Jankoschen Originalarbeit [21], zum Teil einer Folgearbeit von W. Lempken [25] zu entnehmen.

Unter Benutzung der von M. Weller [44] konstruierten treuen Permutationsdarstellung  $\varphi : G \rightarrow S_{173067389}$  wurde zu jedem der 62 oben abgedruckten Konjugiertenklassenvertreterworte  $w$  der Gollan-Ostermann-Vektor  $\mathrm{GO}_M(w)$  bezüglich des Stabilisators

$$M = \mathrm{Stab}_{\varphi(G)}(1) \cong 2^{11} : M_{24}$$

berechnet. Hierzu diente eine parallelrechner-taugliche Implementierung des im Anschluss an Definition 3.6.1 skizzierten Algorithmus, die auf einer von V. Gebhardt (derzeit University of Sydney, Australien; ehemals IEM, Essen) dankenswerterweise zur Verfügung gestellten C++-Klassenbibliothek basiert. Sie benötigte auf 128 Knoten der CRAY-T3E 900/512 im Höchstleistungsrechenzentrum Stuttgart knapp 30 CPU-Stunden, um die verlangten Daten zu produzieren.

Ausgehend von den Gollan-Ostermann-Vektoren konnte schließlich der von  $\varphi$  erzeugte Permutationscharakter  $\pi : G \rightarrow \mathbb{C}$  gemäß Michler und Weller [33] in seine irreduzible Konstituenten zerlegt werden. Es stellte sich heraus, dass  $\pi$  multiplizitätenfrei ist und neben  $\mathbb{1}_G$  noch sechs weitere irreduzible Charaktere der Grade 889111, 1776888, 4290927, 35411145 (zweimal) und 95288172 enthält.

Auf der  $J_4$ -Charaktertafel, die sich in der Charaktertafelbibliothek von GAP befindet, kann nun die Leistungsfähigkeit des beschriebenen Präprozessors zum Dixon-Schneider-Algorithmus getestet werden. Setzen wir alle Zentralisatorordnungen, alle Potenzabbildungen und die sieben Konstituenten von  $\pi$  als bekannt voraus, so fördert ein Durchlauf der Schritte 2–5 bis auf vier alle restlichen Elemente von  $\mathrm{Irr}_{\mathbb{C}}(G)$  zu Tage. Induziert man in Schritt 3 zusätzlich Charaktere aus der maximalen Untergruppe  $M$  von  $G$ , ergibt sich am Ende sogar  $\mathcal{K} = \mathrm{Irr}_{\mathbb{C}}(G)$ .



## Kapitel 4

# Kompatible Charaktere

Aus den speziellen Bedürfnissen einer Anwendung heraus motiviert, wurde der Kompatibilitätsbegriff in Kapitel 2 lediglich für komplexwertige Charaktere eingeführt. Definition 2.2.3 ist jedoch so formuliert, dass sie auch nach der textuellen Ersetzung von  $\mathbb{C}$  durch einen beliebigen endlichen Körper  $\mathbb{F}$  sinnvoll bleibt — selbst dann, wenn die positive Charakteristik von  $\mathbb{F}$  die Ordnung einer der beiden involvierten Gruppen teilt.

Erst auf den zweiten Blick, nämlich im Zusammenhang mit der Konstruktion kompatibler Charakterpaare, wird der herbe Unterschied zwischen klassischer und modularer Darstellungstheorie deutlich.

Bevor wir uns diesem Problem eingehender widmen, soll zunächst ein graphentheoretisches Modell entwickelt werden, das uns zu einem tieferen Verständnis der mit dem Phänomen der Kompatibilität verbundenen Kombinatorik verhilft.

### 4.1 Der Vernetzungsgraph

Seien  $G$  und  $H$  endliche Gruppen sowie  $U \leq G$  und  $V \leq H$  mit  $U \cong V$ . Darüber hinaus sei ein beliebiger Körper  $\mathbb{F}$  gegeben. Ein  $\mathbb{F}$ -Charakter  $\chi$  von  $G$  ist per definitionem genau dann über  $U$  kompatibel zu einem  $\mathbb{F}$ -Charakter  $\vartheta$  von  $H$ , wenn  $\chi \downarrow_U = \vartheta \downarrow_V$  gilt.

Erinnern wir uns daran, wie diese Gleichheitsrelation streng genommen zu lesen ist: Bezüglich einer Identifikation der irreduziblen  $\mathbb{F}$ -Charaktere von  $U$  mit denen von  $V$  setzt sich  $\chi \downarrow_U$  aus den gleichen irreduziblen Konstituenten zusammen wie  $\vartheta \downarrow_V$ . Die Charaktere  $\chi$  und  $\vartheta$  sind im Wesentlichen also über die kleinsten Bestandteile ihrer jeweiligen Restriktionen auf  $U$  bzw.  $V$  miteinander „vernetzt“.

#### Definition 4.1.1 (Menge der irreduziblen Konstituenten)

Sei  $G$  eine endliche Gruppe und  $\mathbb{F}$  ein Körper.

Für einen  $\mathbb{F}$ -Charakter  $\chi$  von  $G$  bzw. einen  $G$ -Modul  $M$  über  $\mathbb{F}$  bezeichne

$$\text{Irr}(\chi) \quad \text{bzw.} \quad \text{Irr}(M)$$

die Menge der irreduziblen Konstituenten von  $\chi$  bzw.  $M$ .

**Bemerkung:** Beim Übergang von  $\chi$  zu  $\text{Irr}(\chi)$  oder von  $M$  zu  $\text{Irr}(M)$  geht die Multiplizität der einzelnen Konstituenten verloren. Diese Information wird auf andere Art in unser Modell einfließen.

Um die Notation nicht unnötig zu komplizieren, gehen wir im Folgenden stets davon aus, dass ein expliziter Isomorphismus  $\alpha$  die Untergruppen  $U$  und  $V$  elementweise identifiziert; insbesondere wird hierdurch eine eindeutige Korrespondenz zwischen den irreduziblen Charakteren bzw. Moduln von  $U$  und  $V$  festgelegt (vergleiche Abschnitt 4.2).

**Definition 4.1.2** (Vernetzungsgraph, (lineare) Ausgeglichenheit)

Seien  $G$  und  $H$  endliche Gruppen, die sich in einer gemeinsamen Untergruppe  $U$  schneiden. Ferner sei  $\mathbb{F}$  ein Körper,  $\chi$  ein  $\mathbb{F}$ -Charakter von  $G$  und  $\vartheta$  ein  $\mathbb{F}$ -Charakter von  $H$ .

Der **Vernetzungsgraph**  $\Upsilon := \Upsilon_U(\chi, \vartheta)$  zu  $\chi$  und  $\vartheta$  über  $U$  besteht aus der Knotenmenge

$$V_\Upsilon = \text{Irr}(\chi) \cup \text{Irr}(\vartheta) \cup \text{Irr}(\chi \downarrow_U) \cup \text{Irr}(\vartheta \downarrow_U),$$

und der gewichteten Kantenmenge

$$E_\Upsilon \subseteq (\text{Irr}(\chi) \times \text{Irr}(\chi \downarrow_U)) \cup (\text{Irr}(\vartheta) \times \text{Irr}(\vartheta \downarrow_U)),$$

wobei eine gerichtete Kante  $(\varphi, \psi)$  genau dann mit dem Gewicht  $m \cdot n \in \mathbb{N}$  versehen in  $E_\Upsilon$  liegt, wenn  $\psi$  ein  $n$ -facher Konstituent von  $\varphi \downarrow_U$  und  $\varphi$  ein  $m$ -facher Konstituent von  $\chi$  oder von  $\vartheta$  ist.

Für jeden Knoten  $v \in \text{Irr}(\chi \downarrow_U) \cup \text{Irr}(\vartheta \downarrow_U)$  bezeichne

$n_G(v)$  die Summe der Gewichte aller Kanten  $(v_G, v) \in E_\Upsilon$ ,  $v_G \in \text{Irr}(\chi)$  und

$n_H(v)$  die Summe der Gewichte aller Kanten  $(v_H, v) \in E_\Upsilon$ ,  $v_H \in \text{Irr}(\vartheta)$ .

Der Graph  $\Upsilon$  heißt **ausgeglichen** bzw. **linear ausgeglichen**, falls

$$n_G(v) = n_H(v) \quad \text{bzw.} \quad n_G(v) = n_H(v) = 1$$

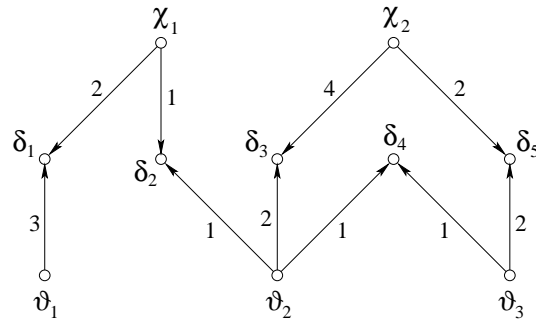
für alle Knoten  $v \in \text{Irr}(\chi \downarrow_U) \cup \text{Irr}(\vartheta \downarrow_U)$ .

Analog definiert man den Vernetzungsgraphen zweier Moduln. Um mit den neuen Begriffen gleich etwas vertrauter zu werden, eignet sich aber wohl eher ein

**Beispiel 4.1.3** *Ein unausgeglichener Vernetzungsgraph.*

Seien die Gruppen  $G$ ,  $H$  und  $U$  wie in Definition 4.1.2 gegeben. Außerdem betrachten wir die Teilmengen  $\{\chi_1, \chi_2\} \subseteq \text{Irr}_{\mathbb{C}}(G)$ ,  $\{\vartheta_1, \vartheta_2, \vartheta_3\} \subseteq \text{Irr}_{\mathbb{C}}(H)$  sowie  $\{\delta_1, \delta_2, \dots, \delta_5\} \subseteq \text{Irr}_{\mathbb{C}}(U)$ , wobei  $\chi_1 \downarrow_U = 2\delta_1 + \delta_2$ ,  $\chi_2 \downarrow_U = 2\delta_3 + \delta_5$  und  $\vartheta_1 \downarrow_U = \delta_1$ ,  $\vartheta_2 \downarrow_U = \delta_2 + 2\delta_3 + \delta_4$ ,  $\vartheta_3 \downarrow_U = \delta_4 + 2\delta_5$  gelte.

Für die  $\mathbb{C}$ -Charaktere  $\chi := \chi_1 + 2\chi_2$  und  $\vartheta := 3\vartheta_1 + \vartheta_2 + \vartheta_3$  sieht dann der Vernetzungsgraph  $\Upsilon := \Upsilon_U(\chi, \vartheta)$  wie folgt aus:



Der Graph  $\Upsilon$  ist nicht ausgeglichen, da etwa  $n_G(\delta_1) = 2 \neq 3 = n_H(\delta_1)$ .



Eine bloße Übersetzung der Definitionen 2.2.3 und 2.2.4 in die Sprache der Graphentheorie liefert zwei wichtige Hilfsaussagen:

**Lemma 4.1.4**

*Es seien  $G$  und  $H$  endliche Gruppen, die sich in einer gemeinsamen Untergruppe  $U$  schneiden. Ferner sei  $\mathbb{F}$  ein Körper,  $\chi$  ein  $\mathbb{F}$ -Charakter von  $G$  und  $\vartheta$  ein  $\mathbb{F}$ -Charakter von  $H$ . Das Paar  $(\chi, \vartheta)$  ist genau dann über  $U$  kompatibel, wenn der Vernetzungsgraph  $\Upsilon_U(\chi, \vartheta)$  ausgeglichen ist.*

**Lemma 4.1.5**

*Es seien  $G$  und  $H$  endliche Gruppen, die sich in einer gemeinsamen Untergruppe  $U$  schneiden. Ferner sei  $\mathbb{F}$  ein Körper. Ein über  $U$  kompatibles Paar  $(\chi, \vartheta)$  von  $\mathbb{F}$ -Charakteren der Gruppen  $G$  respektive  $H$  ist genau dann minimal, wenn der Vernetzungsgraph  $\Upsilon_U(\chi, \vartheta)$  folgender Bedingung genügt:*

*Für alle nicht-leeren, echten Teilmengen  $V \subset \text{Irr}(\chi) \cup \text{Irr}(\vartheta)$ , die samt den von ihren Elementen ausgehenden Kanten aus  $\Upsilon_U(\chi, \vartheta)$  entfernt werden, ist der dabei entstehende Graph unausgeglichen.*

Gerichtete Graphen heißen **schwach zusammenhängend**, falls je zwei ihrer Knoten durch einen ungerichteten Pfad miteinander verbunden sind. In *linear* ausgeglichenen Vernetzungsgraphen ist schwacher Zusammenhang ein hinreichendes Kriterium für die Minimalität des zugrunde liegenden kompatiblen Charakter- bzw. Modulpaares.

**Lemma 4.1.6**

*Es seien  $G$  und  $H$  endliche Gruppen, die sich in einer gemeinsamen Untergruppe  $U$  schneiden. Ferner sei  $\mathbb{F}$  ein Körper,  $\chi$  ein  $\mathbb{F}$ -Charakter von  $G$  und  $\vartheta$  ein  $\mathbb{F}$ -Charakter von  $H$ . Falls der Vernetzungsgraph  $\Upsilon_U(\chi, \vartheta)$  linear ausgeglichen und schwach zusammenhängend ist, ist das Paar  $(\chi, \vartheta)$  über  $U$  kompatibel und minimal.*

**Beweis.** Sei  $\Upsilon := \Upsilon_U(\chi, \vartheta)$ . Nach Lemma 4.1.4 ist  $(\chi, \vartheta)$  über  $U$  kompatibel. Zu zeigen ist daher nur noch die Minimalität dieses Paares.

Angenommen,  $(\chi, \vartheta)$  wäre nicht minimal. Dann gäbe es gemäß Lemma 4.1.5 eine nicht-leere, echte Teilmenge  $V \subset C := \text{Irr}(\chi) \cup \text{Irr}(\vartheta)$ , die samt all den von ihren Elementen ausgehenden Kanten bedenkenlos aus  $\Upsilon$  entfernt werden kann — der entstehende Graph  $\Upsilon'$  wäre nach wie vor ausgeglichen.

Es bezeichne  $V_{\Upsilon'}$  die Knotenmenge von  $\Upsilon'$  und  $n'_G(v)$  sowie  $n'_H(v)$  die zu einem Knoten  $v \in R := \text{Irr}(\chi \downarrow_U) \cup \text{Irr}(\vartheta \downarrow_U) \subset V_{\Upsilon'}$  gehörenden Kantengewichtssummen in  $\Upsilon'$ . Weil  $\Upsilon$  linear ausgeglichen ist, gilt  $n'_G(v), n'_H(v) \in \{0, 1\}$  für alle  $v \in R$ , und wegen  $\emptyset \neq V \neq C$  existieren zwei Knoten  $v_1, v_2 \in R$  mit  $n'_G(v_1) = 1 \neq 0 = n'_G(v_2)$ . Laut Voraussetzung führt in  $\Upsilon$  ein Pfad  $\mathcal{P}$  von  $v_1$  zu  $v_2$ . Dieser Pfad muss jedoch über einen Knoten aus der Eliminationsmenge  $V$  verlaufen, da Knoten aus  $R$  nicht direkt verbunden sein können und von Knoten aus  $C \setminus V$  per Definition von  $\Upsilon'$  keine Kante auf  $v_2$  zeigt. Demnach dürfen wir  $v_1$  ohne Einschränkung so wählen, dass der Sukzessor  $s$  von  $v_1$  in  $\mathcal{P}$  aus  $V$  stammt.

Beim Übergang von  $\Upsilon$  zu  $\Upsilon'$  wurde also eine Kante zwischen  $v_1$  und  $s$  gestrichen. Daraus folgt

$$n_G(v_1) + n_H(v_1) \geq n'_G(v_1) + n'_H(v_1) + 1 = 3,$$

was der linearen Ausgeglichenheit von  $\Upsilon$  widerspricht.  $\square$

## 4.2 Algorithmische Konstruktion kompatibler Charaktere

Lemma 4.1.4 ist der Schlüssel zu einer systematischen Suche nach kompatiblen Paaren. Als methodisches Grundprinzip bietet sich einmal mehr das Backtracking an: Man versuche, die irreduziblen Charaktere zweier Gruppen  $G$  und  $H$  anhand der Informationen über die Zerlegung ihrer jeweiligen Restriktionen auf isomorphe Untergruppen  $U \leq G$  bzw.  $V \leq H$  in jeder denkbaren Weise zu ausgeglichenen Vernetzungsgraphen zu kombinieren.

Um diese Idee praktisch realisieren zu können, fehlen uns momentan noch zwei Details:

1. eine *Datenstruktur*, auf die sich Vernetzungsgraphen oder zumindest ihre wesentlichen Bestandteile abbilden lassen und
2. ein *deterministisches Verfahren* zur Identifikation der irreduziblen Charaktere oder Moduln von  $U$  mit denen von  $V$ .

Eine natürliche und deshalb sehr naheliegende Lösung für Problem Nummer 1 stellen Multimengen dar. Ein Charakter bzw. Modul wird dabei einfach zur Multimenge seiner irreduziblen Konstituenten. Für die Protagonisten von Beispiel 4.1.3 bedeutet das

$$\begin{aligned} \chi &\mapsto \{\chi_1^{(1)}, \chi_2^{(2)}\}, & \vartheta &\mapsto \{\vartheta_1^{(3)}, \vartheta_2^{(1)}, \vartheta_3^{(1)}\}, \\ \chi \downarrow_U &\mapsto \{\delta_1^{(2)}, \delta_2^{(1)}, \delta_3^{(4)}, \delta_5^{(2)}\}, & \vartheta \downarrow_U &\mapsto \{\delta_1^{(3)}, \delta_2^{(1)}, \delta_3^{(2)}, \delta_4^{(2)}, \delta_5^{(2)}\}. \end{aligned}$$

Ausgeglichene Vernetzungsgraphen werden unter dieser Lesart zu gleichen Multimengen.

Für die Lösung des Problems Nummer 2 ist ein konkreter Isomorphismus  $\alpha : U \rightarrow V$  absolut unabdingbar. Wie in Kapitel 2 skizziert, erklären wir eine einmal fest vereinbarte Reihenfolge der Konjugiertenklassen von  $U$  zum Standard, übertragen ein Repräsentantensystem  $\mathcal{S}$  für ebendiese Klassen vermöge  $\alpha$  nach  $V$  und können dort dann jeden irreduziblen Charakter durch Auswertung (bzw. jeden irreduziblen Modul durch Bildung der Spur seiner assoziierten Darstellung) auf dem Bild  $\alpha(\mathcal{S})$  eindeutig einem über  $U$  definierten Pendant zuordnen.

Im Anschluss daran ist es möglich, die Restriktionen der irreduziblen Charaktere (bzw. Moduln) von  $G$  auf  $U$  und die Restriktionen der irreduziblen Charaktere (bzw. Moduln) von  $H$  auf  $V$  bezüglich einer gemeinsamen Basis in irreduzible Konstituenten zu zerlegen.

### Algorithmus 4.2.1 (konsistente Restriktionszerlegung, Version für $\mathbb{C}$ -Charaktere)

Seien  $G$  und  $H$  Permutationsgruppen sowie  $U \leq G$  und  $V \leq H$  mit  $U \cong V$ . Ferner seien ein Isomorphismus  $\alpha : U \rightarrow V$ , ein geordnetes Vertretersystem  $\mathcal{S}$  für die Konjugiertenklassen von  $U$  sowie konkrete Charaktertafeln für  $G$ ,  $H$ ,  $U$  und  $V$  gegeben.

#### **Schritt 1**

Ordne die Spalten der Charaktertafel von  $U$  so an, dass die neue  $j$ -te Spalte die Werte der irreduziblen Charaktere von  $U$  auf dem  $j$ -ten Element von  $\mathcal{S}$  enthält,  $1 \leq j \leq |\mathcal{S}|$ .  
 Ordne die Spalten der Charaktertafel von  $V$  so an, dass die neue  $j$ -te Spalte die Werte der irreduziblen Charaktere von  $U$  auf dem  $j$ -ten Element von  $\alpha(\mathcal{S})$  enthält,  $1 \leq j \leq |\mathcal{S}|$ .  
 Bringe nun die Charaktertafel von  $V$  durch Zeilenvertauschungen mit der Charaktertafel von  $U$  zur Deckung.

**Schritt 2**

Initialisiere die Zerlegungsdatenliste  $X := [ ]$ .  
**Für**  $\chi \in \text{Irr}_{\mathbb{C}}(G)$  :  
 Initialisiere die Restriktionsmultimenge  $R(\chi) := \emptyset$ .  
**Für**  $\delta \in \text{Irr}_{\mathbb{C}}(U) = \text{Irr}_{\mathbb{C}}(V)$  :  
 Berechne die Multiplizität  $m := [\chi \downarrow_U, \delta]_U$ .  
**Falls**  $m \neq 0$  :  
 Setze  $R(\chi) := R(\chi) \uplus \{\delta^{(m)}\}$  /\* Multimengenvereinigung! \*/  
 Setze  $X := X \cup [R(\chi)]$ .

**Schritt 3**

Initialisiere die Zerlegungsdatenliste  $T := [ ]$ .  
**Für**  $\vartheta \in \text{Irr}_{\mathbb{C}}(H)$  :  
 Initialisiere die Restriktionsmultimenge  $R(\vartheta) := \emptyset$ .  
**Für**  $\delta \in \text{Irr}_{\mathbb{C}}(V) = \text{Irr}_{\mathbb{C}}(U)$  :  
 Berechne die Multiplizität  $m := [\vartheta \downarrow_V, \delta]_V$ .  
**Falls**  $m \neq 0$  :  
 Setze  $R(\vartheta) := R(\vartheta) \uplus \{\delta^{(m)}\}$   
 Setze  $T := T \cup [R(\vartheta)]$ .

**Ende**

Die so ermittelten Listen  $X$  und  $T$  von Multimengen dienen später als Eingabe für die eigentliche Backtracking-Prozedur. Bleibt die Frage zu klären, wie man über einem Körper  $\mathbb{F}$  mit positiver Charakteristik  $p$  vorzugehen hat, wo das innere Produkt von Charakteren entweder nicht definiert ist (falls nämlich  $p$  die Gruppenordnung  $|U| = |V|$  teilt) oder die Multiplizität eines irreduziblen Arguments nur modulo  $p$  liefert.

Angesichts derart widriger Umstände erscheint es zweckmäßig, auf die Modulebene zurückzuweichen. Statt der Charaktertafeln von  $G$ ,  $H$ ,  $U$  und  $V$  benötigen wir dazu Repräsentanten aller irreduziblen Moduln dieser Gruppen über  $\mathbb{F}$ ; der Dekompositionskalkül beruht dann auf R. A. Parkers MEAT-AXE [34].

Komponentenweise Addition zweier kompatibler Charakterpaare ergibt offenkundig wieder ein kompatibles Paar. Diese Abgeschlossenheitseigenschaft lenkt unser Interesse auf *minimale* Paare und lässt erahnen, wie mächtig die Menge *aller* kompatiblen Paare zu einem vorgegebenen Quadrupel  $(G, H, U, V)$  von Gruppen bzw. isomorphen Untergruppen im Allgemeinen ist. Um sie algorithmisch kontrollieren zu können, müssen wir sie daher geeignet unterteilen.

**Definition 4.2.2 (Sollkonstituent)**

Seien  $G$  und  $H$  endliche Gruppen sowie  $U \leq G$  und  $V \leq H$  mit  $U \cong V$ . Darüber hinaus sei  $\mathbb{F}$  ein beliebiger Körper und  $\Pi$  die Menge aller über  $U$  kompatiblen Paare von  $\mathbb{F}$ -Charakteren der Gruppen  $G$  respektive  $H$ .

Für jede natürliche Zahl  $d \in \mathbb{N}$  und jeden irreduziblen  $\mathbb{F}$ -Charakter  $\xi$  von  $G$  bzw.  $H$  bezeichne

$$\Pi_{G,\xi}^{\leq d} := \{(\chi, \vartheta) \in \Pi \mid \deg(\chi, \vartheta) \leq d, \xi \text{ ist Konstituent von } \chi\}$$

$$\text{bzw. } \Pi_{H,\xi}^{\leq d} := \{(\chi, \vartheta) \in \Pi \mid \deg(\chi, \vartheta) \leq d, \xi \text{ ist Konstituent von } \vartheta\}$$

die Menge aller über  $U$  kompatiblen Paare mit **Sollkonstituent**  $\xi$  und maximalem Grad  $d$ .

Analog definiert man den Sollkonstituenten eines über  $U$  kompatiblen Modulpaares, wobei der Begriff des Charaktergrades freilich durch den der Moduldimension zu substituieren ist. Um den Textfluss nicht der formalen Korrektheit opfern zu müssen, wird im Folgenden allerdings ausschließlich von  $\mathbb{C}$ -Charakteren die Rede sein.

In Anwendungen suchen wir typischerweise nach kompatiblen Paaren, deren erste bzw. zweite Komponente eine gewisse Konjugiertenklasse von  $G$  bzw.  $H$  *nicht* im Kern hat. Meist erfüllen nur relativ wenige irreduzible Charaktere  $\xi$  der betreffenden Gruppe diese Anforderung. Die Gesamtlösungsmenge wird aufgrund dessen am besten als Vereinigung von Teillösungsmengen mit den entsprechenden Sollkonstituenten  $\xi$  gewonnen.

Ein Verfahren zur Konstruktion der Mengen  $\Pi_{G,\xi}^{\leq d}$  bzw.  $\Pi_{H,\xi}^{\leq d}$  aus Definition 4.2.2 kann nun die Zerlegungsdaten des Sollkonstituenten als Fundament nutzen: Die irreduziblen Bestandteile der Restriktion  $\xi \downarrow_U$  bzw.  $\xi \downarrow_V$  geben bestimmte **Ziele** vor, sprich unausgeglichene Knoten im aufzubauenden Vernetzungsgraphen  $\Upsilon := \Upsilon_U(\xi + ?, ?)$  bzw.  $\Upsilon := \Upsilon_U(?, \xi + ?)$ . Aus dem **Pool** der irreduziblen Charaktere von  $H$  bzw.  $G$  filtern wir uns sodann diejenigen Elemente heraus, welche die vorgegebenen Ziele **treffen**, das heißt deren Restriktion auf  $U \cong V$  mindestens einen Konstituenten mit  $\xi \downarrow_U$  bzw.  $\xi \downarrow_V$  gemein hat.

Dieser Menge von **Alternativen** entnehmen wir so lange Konstituenten, bis sämtliche durch  $\xi \downarrow_U$  bzw.  $\xi \downarrow_V$  definierten Ziele getroffen wurden. Falls infolge unserer Wahl keine neuen Ziele entstanden sind, liegt am Ende ein ausgeglichener Vernetzungsgraph  $\Upsilon$ , laut Lemma 4.1.4 also ein kompatibles Paar vor. Ansonsten iterieren wir den Konstruktionsprozess mit jeweils vertauschtem Pool, bis die Gradschranke  $d$  überschritten oder die Menge der aktuellen Alternativen leer ist. Dann sind Wahlentscheidungen auf vorausgegangenen Levels zu stornieren und sukzessive durch eventuell noch verbliebene Alternativen zu ersetzen.

**Algorithmus 4.2.3** (kompatible Paare mit Sollkonstituent und maximalem Grad)

Seien  $G$  und  $H$  Permutationsgruppen sowie  $U \leq G$  und  $V \leq H$  mit  $U \cong V$ . Ferner seien die mit Hilfe von Algorithmus 4.2.1 produzierten Zerlegungsdatenlisten  $X$  und  $T$ , der gewünschte Sollkonstituent  $\xi$ , die Gradschranke  $d \in \mathbb{N}$  sowie konkrete Charaktertafeln für  $G$  und  $H$  gegeben.

**Schritt 1**

Stelle die Liste  $d_X$  der Grade aller Elemente von  $\text{Irr}_{\mathbb{C}}(G)$  auf, so dass  $d_T[i]$  gerade der Grad des Charakters  $\chi$  mit Restriktion  $\chi \downarrow_U = X[i]$  ist.

Stelle die Liste  $d_T$  der Grade aller Elemente von  $\text{Irr}_{\mathbb{C}}(H)$  auf, so dass  $d_T[i]$  gerade der Grad des Charakters  $\vartheta$  mit Restriktion  $\vartheta \downarrow_V = T[i]$  ist.

**Schritt 2**

**Falls**  $\xi \in \text{Irr}_{\mathbb{C}}(G)$  :

Bestimme den Index  $i$  mit  $\xi \downarrow_U = X[i]$ .

Initialisiere das Zieleprotokoll  $Z := [X[i], \emptyset]$ .

Initialisiere das Zusatztrefferprotokoll  $Z_{\text{neu}} := [\emptyset, X[i]]$ .

Initialisiere das Poolprotokoll  $P := [X]$ .

Initialisiere die Multimenge  $M(\chi) := \{\xi^{(1)}\}$

und den Kontrollgrad  $d_\chi = \chi(1_G) := d_X[i]$ .

Initialisiere die Multimenge  $M(\vartheta) := \emptyset$

und den Kontrollgrad  $d_\vartheta = \vartheta(1_H) := 0$ .

**Sonst :**

Bestimme den Index  $i$  mit  $\xi \downarrow_V = T[i]$ .  
 Initialisiere das Zieleprotokoll  $Z := [T[i], \emptyset]$ .  
 Initialisiere das Zusatztrefferprotokoll  $Z_{\text{neu}} := [\emptyset, T[i]]$ .  
 Initialisiere das Poolprotokoll  $P := [T]$ .  
 Initialisiere die Multimenge  $M(\chi) := \emptyset$   
 und den Kontrollgrad  $d_\chi = \chi(1_G) := 0$ .  
 Initialisiere die Multimenge  $M(\vartheta) := \{\xi^{(1)}\}$   
 und den Kontrollgrad  $d_\vartheta = \vartheta(1_H) := d_T[i]$ .  
 Initialisiere das Wahlprotokoll  $W := [i]$ .  
 Initialisiere das Alternativenprotokoll  $A := [[\ ]]$ .  
 Initialisiere die Ergebnismenge  $K := \emptyset$ .  
 Setze den aktuellen Level  $\ell := 2$  und die letzte Aktion  $a := \text{„track“}$ .

**Schritt 3****Solange  $\ell \neq 1$  :**

**Falls**  $a = \text{„track“}$  und  $Z[\ell] = \emptyset$  und  $Z_{\text{neu}}[\ell] = \emptyset$  :  
 /\* Dann sind durch die Wahl auf Level  $\ell - 1$  sämtliche offenen Ziele getroffen \*/  
 /\* worden, das heißt  $\chi$  ist über  $U$  kompatibel zu  $\vartheta$ . \*/  
 Setze  $K := K \cup \{(M(\chi), M(\vartheta))\}$ .  
 Dekrementiere  $\ell$  um 1 und setze  $a := \text{„back“}$ .  
**Falls hingegen**  $a = \text{„track“}$  und  $Z[\ell] = \emptyset$  und  $Z_{\text{neu}}[\ell] \neq \emptyset$  :  
 /\* Dann wurde durch die Wahl auf Level  $\ell - 1$  das letzte offene Ziel für Kon- \*/  
 /\* stituenten aus dem Pool  $P[\ell - 1]$  getroffen, aufgrund von Zusatztreffern sind \*/  
 /\* aber noch Ziele für Konstituenten aus dem anderen möglichen Pool offen. \*/  
**Falls**  $P[\ell - 1] = X$  :  
 Setze  $P[\ell] := T$ .  
**Sonst :**  
 Setze  $P[\ell] := X$ .  
 Setze  $Z[\ell] := Z_{\text{neu}}[\ell]$  und setze  $Z_{\text{neu}}[\ell] := \emptyset$ .  
**Falls hingegen**  $a = \text{„track“}$  und  $Z[\ell] \neq \emptyset$  :  
 /\* Dann sind noch Ziele für Konstituenten aus dem Pool  $P[\ell]$  offen. \*/  
**Falls**  $P[\ell] = X$  :  
 Initialisiere  $A[\ell] := [j \in \{1, 2, \dots, |X|\} \mid d_\chi + d_X[j] \leq d, X[j] \cap Z[\ell] \neq \emptyset]$ .  
**Sonst :**  
 Initialisiere  $A[\ell] := [j \in \{1, 2, \dots, |T|\} \mid d_\vartheta + d_T[j] \leq d, T[j] \cap Z[\ell] \neq \emptyset]$ .  
**Falls**  $A[\ell] = [\ ]$  : /\* Keine Fortsetzung mehr möglich \*/  
 Dekrementiere  $\ell$  um 1 und setze  $a := \text{„back“}$ .  
**Sonst :**  
 Streiche den letzten Eintrag  $k$  aus  $A[\ell]$ .  
 Setze  $W[\ell] := k$ .  
**Falls**  $P[\ell] = X$  :  
 Bestimme den Charakter  $\varphi$  mit  $\varphi \downarrow_U = P[\ell][k]$ .  
 Setze  $M(\chi) := M(\chi) \uplus \{\varphi^{(1)}\}$ .  
 Inkrementiere  $d_\chi$  um  $d_X[k]$ .

**Sonst :**

Bestimme den Charakter  $\psi$  mit  $\psi \downarrow_V = P[\ell][k]$ .

Setze  $M(\vartheta) := M(\vartheta) \uplus \{\psi^{(1)}\}$ .

Inkrementiere  $d_\vartheta$  um  $d_T[k]$ .

Setze  $Z[\ell + 1] := Z[\ell] \setminus P[\ell][k]$ . /\* Multimengendifferenz! \*/

Setze  $Z_{\text{neu}}[\ell + 1] := Z_{\text{neu}}[\ell] \uplus (P[\ell][k] \setminus Z[\ell])$ .

Setze  $P[\ell + 1] := P[\ell]$ .

Inkrementiere  $\ell$  um 1 und setze  $a := \text{„track“}$ .

**Sonst :**

/\* Dann gilt  $a = \text{„back“}$ , das heißt alle sich aus der zuletzt auf Level  $\ell$  getroffenen \*/

/\* Wahl ergebenden Möglichkeiten wurden komplett durchgespielt. \*/

Setze  $k := W[\ell]$ .

**Falls**  $P[\ell] = X$  :

Bestimme den Charakter  $\varphi$  mit  $\varphi \downarrow_U = P[\ell][k]$ .

Setze  $M(\chi) := M(\chi) \setminus \{\varphi^{(1)}\}$ .

Dekrementiere  $d_\chi$  um  $d_X[k]$ .

**Sonst :**

Bestimme den Charakter  $\psi$  mit  $\psi \downarrow_V = P[\ell][k]$ .

Setze  $M(\vartheta) := M(\vartheta) \setminus \{\psi^{(1)}\}$ .

Dekrementiere  $d_\vartheta$  um  $d_T[k]$ .

**Falls**  $A[\ell] = []$  : /\* Keine Alternativen mehr übrig \*/

Dekrementiere  $\ell$  um 1 und setze  $a := \text{„back“}$ .

**Sonst :**

Streiche den letzten Eintrag  $k$  aus  $A[\ell]$ .

Setze  $W[\ell] := k$ .

**Falls**  $P[\ell] = X$  :

Bestimme den Charakter  $\varphi$  mit  $\varphi \downarrow_U = P[\ell][k]$ .

Setze  $M(\chi) := M(\chi) \uplus \{\varphi^{(1)}\}$ .

Inkrementiere  $d_\chi$  um  $d_X[k]$ .

**Sonst :**

Bestimme den Charakter  $\psi$  mit  $\psi \downarrow_V = P[\ell][k]$ .

Setze  $M(\vartheta) := M(\vartheta) \uplus \{\psi^{(1)}\}$ .

Inkrementiere  $d_\vartheta$  um  $d_T[k]$ .

Setze  $Z[\ell + 1] := Z[\ell] \setminus P[\ell][k]$ .

Setze  $Z_{\text{neu}}[\ell + 1] := Z_{\text{neu}}[\ell] \uplus (P[\ell][k] \setminus Z[\ell])$ .

Setze  $P[\ell + 1] := P[\ell]$ .

Inkrementiere  $\ell$  um 1 und setze  $a := \text{„track“}$ .

<b>Ende</b>
-------------

Zur Ermittlung der Alternativenliste  $A[\ell]$  auf Level  $\ell$  können zusätzlich auch noch diverse optionale Einschränkungen herangezogen werden. Denkbar ist beispielsweise, dass wir lediglich nach kompatiblen Paaren mit multiplizitätenfreien Komponenten suchen wollen: Neben den Gradlisten  $d_X$  und  $d_T$  wären hierfür einfach Bitfelder  $used_X$  oder/und  $used_T$  der Länge  $|X|$  bzw.  $|T|$  zu verwalten, in denen das  $i$ -te Bit genau dann gesetzt ist, wenn sich der irreduzible Charakter mit Restriktion  $X[i]$  bzw.  $T[i]$  schon in der Multimenge  $M(\chi)$  bzw.  $M(\vartheta)$  befindet.

**Satz 4.2.4**

Angewandt auf zwei Permutationsgruppen  $G$  und  $H$  mit zueinander isomorphen Untergruppen  $U \leq G$  und  $V \leq H$ , einen Sollkonstituenten  $\xi$  sowie eine Gradschranke  $d \in \mathbb{N}$  terminiert Algorithmus 4.2.3. Für die resultierende Menge  $K$  gilt

$$K \subseteq \Pi_0 := \begin{cases} \Pi_{G,\xi}^{\leq d}, & \text{falls } \xi \in \text{Irr}_{\mathbb{C}}(G), \\ \Pi_{H,\xi}^{\leq d}, & \text{falls } \xi \in \text{Irr}_{\mathbb{C}}(H), \end{cases}$$

und alle in  $\Pi_0 \setminus K$  enthaltenen über  $U$  kompatiblen Paare sind nicht minimal.

**Beweis.** Auf jedem mit der Aktion „track“ erreichten Level  $\ell$  berechnet Algorithmus 4.2.3 eine endliche Liste  $A[\ell]$  von als Konstituent in Frage kommenden Charakteren. Durch die Gradschranke  $d$  ist gewährleistet, dass dieser Schritt schlimmstenfalls bis zu Level  $2d$  wiederholt werden muss, weil pro Level entweder der Grad  $d_\chi$  oder der Grad  $d_\vartheta$  um mindestens 1 inkrementiert wird. Demzufolge bestehen auf endlich vielen Levels endlich oft endlich viele Verzweigungsmöglichkeiten, das heißt Algorithmus 4.2.3 terminiert.

Wie bereits im Verfahrensentwurf erläutert wurde, ist die Inklusion  $K \subseteq \Pi_0$  eine direkte Konsequenz aus Lemma 4.1.4.

Sei abschließend  $(\chi, \vartheta) \in \Pi_0 \setminus K$ . Da Algorithmus 4.2.3 per Konstruktionsprinzip jeden schwach zusammenhängenden Vernetzungsbaum über dem Knoten  $\xi$  samt seinen Restriktionen auf  $U$  bzw.  $V$  errichtet und diesen Prozess genau dann vor Ausschöpfung aller Kombinationsmöglichkeiten abbricht, wenn ein ausgeglichener Vernetzungsbaum vorliegt, existiert in  $\text{Irr}(\chi) \cup \text{Irr}(\vartheta)$  offenbar eine nicht-leere, echte Teilmenge, die man zusammen mit den von ihren Elementen ausgehenden Kanten aus  $\Upsilon_U(\chi, \vartheta)$  entfernen kann, ohne die Eigenschaft der Ausgeglichenheit zu verletzen. Nach Lemma 4.1.5 ist  $(\chi, \vartheta)$  deshalb nicht minimal.  $\square$

Zu Lemma 4.1.6 ergibt sich aus dem vorangegangenen Beweis ein wichtiges

**Korollar 4.2.5**

Es seien  $G$  und  $H$  Permutationsgruppen sowie  $U \leq G$  und  $V \leq H$  mit  $U \cong V$ . Ferner sei  $(\chi, \vartheta)$  ein mit Algorithmus 4.2.3 konstruiertes, über  $U$  kompatibles  $\mathbb{C}$ -Charakterpaar. Dann gilt: Ist die gemeinsame Restriktion  $\chi|_U = \vartheta|_V$  multiplizitätenfrei, so ist das Paar  $(\chi, \vartheta)$  minimal.

**Beweis.** Laut Voraussetzung ist  $\Upsilon_U(\chi, \vartheta)$  linear ausgeglichen. Da Algorithmus 4.2.3 nur schwach zusammenhängende Vernetzungsgraphen aufbaut, folgt die Minimalität des Paares  $(\chi, \vartheta)$  aus Lemma 4.1.6.  $\square$

## 4.3 Implementierung und qualitatives Laufzeitverhalten

Die Tatsache, dass MAGMA [2] in Gestalt von `SetMulti` einen „hauseigenen“ Multimengen-Datentyp zur Verfügung stellt, gab den Ausschlag, Algorithmus 4.2.3 vorläufig bloß für dieses Computeralgebrasystem zu implementieren.

Der gesamte zugehörige Programmcode ist gemäß den Richtlinien der GNU General Public License<sup>1</sup> frei verfügbar und befindet sich im Format eines (unkomprimierten) **tar**-Archivs auf der beiliegenden Diskette. Eine Installationsbeschreibung ist Abschnitt 3.5 zu entnehmen.

### 4.3.1 Die Funktionen der scp-Bibliothek

Nach dem Einlesen der Datei **scp.mag** in eine MAGMA-Sitzung kennt das System jede der im Folgenden dokumentierten Funktionen.

**MultisetDifference(  $ms_1$ ,  $ms_2$  ) :**

berechnet die Multimengendifferenz  $ms_1 \setminus ms_2$ .

**RestrictionsOnIsomorphicSubgroups(  $ct_1$ ,  $cts_1$ ,  $ccs_1$ ,  $ct_2$ ,  $cts_2$ ,  $ccs_2$  ) :**

berechnet die Zerlegungen aller auf isomorphe Untergruppen  $U \leq G$  bzw.  $V \leq H$  mit Charaktertafel  $cts_1$  bzw.  $cts_2$  restringierten Zeilen der Charaktertafeln  $ct_1$  (Gruppe  $G$ ) und  $ct_2$  (Gruppe  $H$ ) in irreduzible Konstituenten. Die Konjugiertenklassenvertretersequenzen  $ccs_1$  (für  $U$ ) und  $ccs_2$  (für  $V$ ) werden benötigt, um Konsistenz zwischen der Charakterreihenfolge in  $cts_1$  und  $cts_2$  zu erwirken.

Die Funktion liefert drei Rückgabewerte:

1. die Zerlegungsdatenliste  $X$  gemäß Algorithmus 4.2.1;
2. die Zerlegungsdatenliste  $T$  gemäß Algorithmus 4.2.1;
3. die Zeilenpermutation, welche auf die Tafel  $cts_2$  angewendet werden muss, um sie mit der Tafel  $cts_1$  zur Deckung zu bringen.

**RestrictionsOnIsomorphicSubgroups\_MOD(  $mds_1$ ,  $mdss_1$ ,  $ccs_1$ ,  $mds_2$ ,  $mdss_2$ ,  $ccs_2$  ) :**

berechnet die Zerlegungen aller auf isomorphe Untergruppen  $U \leq G$  bzw.  $V \leq H$  mit Modulsystem  $mdss_1$  bzw.  $mdss_2$  restringierten Elemente der Modulsysteme  $mds_1$  (Gruppe  $G$ ) und  $mds_2$  (Gruppe  $H$ ) in irreduzible Konstituenten. Die Konjugiertenklassenvertretersequenzen  $ccs_1$  (für  $U$ ) und  $ccs_2$  (für  $V$ ) werden benötigt, um Konsistenz zwischen der Modulreihenfolge in  $mdss_1$  und  $mdss_2$  zu erwirken.

Die Funktion liefert drei Rückgabewerte:

1. die Zerlegungsdatenliste  $X$  gemäß Algorithmus 4.2.1;
2. die Zerlegungsdatenliste  $T$  gemäß Algorithmus 4.2.1;
3. die Indexpermutation, welche auf das System  $mdss_2$  angewendet werden muss, um es bezüglich Isomorphie in dieselbe Reihenfolge wie das System  $mdss_1$  zu bringen.

**SearchCompatiblePairs(  $ct_1$ ,  $ct_2$ ,  $cts$ ,  $X$ ,  $T$ ,  $mf_1$ ,  $mf_2$ ,  $mfs$ ,  $d$ ,  $ip$ ,  $ic$  ) :**

bestimmt die Menge  $\Pi_{G,\xi}^{\leq d}$  bzw.  $\Pi_{H,\xi}^{\leq d}$  für eine Gruppe  $G$  mit Charaktertafel  $ct_1$  und eine Gruppe  $H$  mit Charaktertafel  $ct_2$ , die isomorphe Untergruppen  $U \cong V$  mit Charaktertafel  $cts$  besitzen. Weitere Eingabeparameter sind:

- die Zerlegungsdatenliste  $X$  gemäß Algorithmus 4.2.1;
- die Zerlegungsdatenliste  $T$  gemäß Algorithmus 4.2.1;
- das Flag  $mf_1$ ; auf **true** zu setzen, wenn nur multiplizitätenfreie Charaktere  $\chi$  von  $G$  als Komponente eines über  $U$  kompatiblen Paares  $(\chi, \vartheta)$  erwünscht sind.

---

<sup>1</sup>Siehe **gnugpl.txt** auf der beiliegenden Diskette oder <http://www.gnu.org/copyleft/gpl.html> .



- das Flag  $mf_2$ ; auf **true** zu setzen, wenn nur multiplizitätenfreie Charaktere  $\vartheta$  von  $H$  als Komponente eines über  $U$  kompatiblen Paares  $(\chi, \vartheta)$  erwünscht sind.
- das Flag  $mfs$ ; auf **true** zu setzen, wenn ausschließlich nach über  $U$  kompatiblen Paaren  $(\chi, \vartheta)$  mit multiplizitätenfreier gemeinsamer Restriktion  $\chi|_U = \vartheta|_U$  gesucht werden soll.
- das Flag  $ip$ ; auf  $i$  zu setzen, falls der Sollkonstituent  $\xi$  aus der Charaktertafel  $ct_i$  stammt ( $i = 1, 2$ ).
- der Index  $ic$  des Sollkonstituenten  $\xi$  in seiner Charaktertafel.

**SearchCompatiblePairs\_MOD**(  $d_X, d_T, X, T, mf_1, mf_2, mfs, d, ip, ic$  ) :

bestimmt über einem Körper  $\mathbb{F}$  mit positiver Charakteristik die Menge  $\Pi_{G,Y}^{\leq d}$  bzw.  $\Pi_{H,Y}^{\leq d}$  für eine Gruppe  $G$  mit irreduziblen Moduln der  $\mathbb{F}$ -Dimensionen  $d_X$  und eine Gruppe  $H$  mit irreduziblen Moduln der  $\mathbb{F}$ -Dimensionen  $d_T$ , die isomorphe Untergruppen besitzen. Alle übrigen Eingabeparameter sind analog zur Funktion **SearchCompatiblePairs** zu verstehen.

Um dem Benutzer mühseliges Nachrechnen zu ersparen, sind die Elemente der von den Funktionen **SearchCompatiblePairs** und **SearchCompatiblePairs\_MOD** produzierten Mengen in Wahrheit Tripel, deren dritte Komponente den Grad des von den ersten beiden gebildeten kompatiblen Paares wiedergibt.

#### 4.3.2 Bemerkungen zur Komplexität

Abermals steht ein Backtracking-Verfahren zur Debatte und wie schon in Kapitel 3 entzieht es sich jeder quantitativen Komplexitätsanalyse, die mit rein elementaren Mitteln geführt werden könnte.

Zweifelsohne hängt die für Algorithmus 4.2.3 zu erwartende Laufzeit signifikant von der gewählten Gradschranke  $d$  ab — oder präziser formuliert von der Differenz zwischen  $d$  und dem Grad des Sollkonstituenten  $\xi$ . Je größer dieser Unterschied ausfällt, desto mehr Spielraum bleibt für die Wahl weiterer Konstituenten. Entscheidend ist jedoch nicht allein die Größe des Spielraums, sondern vielmehr die Anzahl seiner möglichen Partitionierungen: Wieviele Alternativen lassen sich finden, um ein konkretes Ziel zu treffen?

Diese Frage entbehrt einer generell gültigen Antwort, denn sie ist äquivalent zur Frage nach gewissen Knotenvalenzen in einem Vernetzungsgraphen, der nicht zuletzt von der Struktur der beteiligten Gruppen  $G, H, U$  und  $V$  bestimmt wird. Der potentiell schlimmste Fall liegt vor, wenn  $U \cong V$  abelsch ist und großen Index in den nicht-abelschen Gruppen  $G$  bzw.  $H$  aufweist. Dann zerfallen die Restriktionen der irreduziblen Charaktere oder Moduln von  $G$  und  $H$  in eine Unmenge von linearen respektive eindimensionalen Konstituenten.

Anwendungen im Rahmen des Michler-Algorithmus, der diese extreme Situation a priori zu vermeiden sucht (siehe Kapitel 2), sind in der Regel unkritisch, zumal hier primär nach kompatiblen Paaren *minimalen Grades* gesucht wird.



## Kapitel 5

# Ein Existenzbeweis für die Rudvalis-Gruppe

Im Jahre 1972 fand A. Rudvalis [37] handfeste Hinweise auf eine neue sporadische einfache Gruppe der Ordnung

$$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29 = 145926144000$$

als er einen speziellen 3-partiten und 2304-regulären Graphen  $\Gamma$  mit 4060 Knoten sowie dessen Automorphismengruppe  $\text{Aut}(\Gamma)$  studierte. Keine neun Monate später gelang J. H. Conway und D. B. Wales [7] der erste wirkliche Existenzbeweis für die bereits von ihnen so bezeichnete „Rudvalis-Gruppe“, die heutzutage mit dem Standardkürzel Ru symbolisiert wird.

Während Conway und Wales in ihrer Arbeit die eindeutig bestimmte Rang-3-Erweiterung der Ree-Gruppe  ${}^2F_4(2)$  konstruierten, eröffnet uns der Michler-Algorithmus einen völlig anderen Zugang — vorausgesetzt wir kennen den Zentralisator einer 2-zentralen Involution in Ru!

### 5.1 Von der 2-Sylowuntergruppe zum Zentralisator

Auf der Suche nach einem „geeigneten“ Eingabeparameter für den Michler-Algorithmus weist eine entsprechende Charakterisierung der Rudvalis-Gruppe von D. Parrot [35] den Weg.

**Satz 5.1.1 (PARROT)**

*Es sei  $G$  eine endliche Gruppe sowie  $z \in G$  eine 2-zentrale Involution derart, dass  $H := \mathbf{C}_G(z)$  den folgenden drei Bedingungen genügt:*

- (i)  $J := O_2(H)$  hat die Ordnung  $2^{11}$  und Nilpotenzklasse  $c(J) \geq 3$ ;
- (ii)  $H/J \cong S_5$ ;
- (iii)  $Q \in \text{Syl}_3(H) \implies \mathbf{C}_J(Q) \cong Q_8$ .

*Dann gilt  $G = H.O(G)$  oder  $G \cong \text{Ru}$ .*

Parrot beginnt den Beweis dieses Satzes mit einer Analyse der Struktur von  $H$ . Unter anderem gewinnt er dabei wesentlich genauere Informationen über den maximalen 2-Normalteiler  $J$ . Der bequemen Zitierbarkeit halber notieren wir eine Zusammenfassung der Aussagen von Lemma 1 und 2 in [35].

**Lemma 5.1.2**

Unter den Voraussetzungen von Satz 5.1.1 gelten:

- (a)  $J$  enthält einen elementar abelschen Normalteiler  $E$  der Ordnung  $|E| = 2^5$ , welcher sogar normal in  $H$  ist.
- (b)  $\mathbf{C}_G(E) = \mathbf{C}_J(E) \cong 2^4 \times \mathbf{Q}_8$ , insbesondere ist  $E < \mathbf{C}_J(E)$ ;
- (c)  $E = J' = \Phi(J)$ ;
- (d)  $\mathbf{Z}(J) = [J, J'] = \mathbf{Z}(H) = \langle z \rangle$ ;
- (e)  $J$  hat Nilpotenzklasse  $c(J) = 3$ .

Freilich lässt sich damit alleine noch kein Involutionenzentralisator in  $\text{Ru}$  bauen. Aber diese Daten sind, um im Bild zu bleiben, der Grundriss für jedes Konstrukt, das auf dem im vierten Abschnitt von [35] gegossenen Fundament errichtet werden kann:

**Satz 5.1.3 (PARROT)**

Es sei  $G$  eine endliche Gruppe sowie  $z \in G$  eine 2-zentrale Involution derart, dass  $H := \mathbf{C}_G(z)$  den Bedingungen (i)–(iii) aus Satz 5.1.1 genügt. Ferner sei  $S \in \text{Syl}_2(H)$  mit  $z \in \mathbf{Z}(S)$ . Dann ist  $S$  isomorph zu einer Faktorgruppe der freien Gruppe über

$$\mathcal{X} := \{ z, t, v, w, w_1, x_1, x_2, a, b, c, d, y, y_2, u \}$$

und besitzt die endliche Präsentation  $S = \langle \mathcal{X} \mid \mathcal{S} \rangle$ , wobei sich die Relationenmenge  $\mathcal{S}$  aus den Ordnungsgleichungen

$$g^2 = 1 \text{ für } g \in \mathcal{X} \setminus \{x_1, x_2\} \quad \text{bzw.} \quad x_1^2 = x_2^2 = z$$

sowie aus den paarweisen Kommutatoren  $[g, h]$ ,  $g, h \in \mathcal{X}$  zusammensetzt, die bis auf folgende Ausnahmen alle trivial sind:

$$\begin{aligned} [t, d] &= [v, c] = [w, b] = [w_1, a] = [x_1, x_2] = [u, x_1] = [x_2, y] = z, \\ [v, u] &= [w, y] = [a, x_1] = [a, y_2] = t, \quad [b, x_1] = v, \\ [w_1, u] &= [c, x_1] = [a, d] = w, \quad [d, x_1] = [b, c] = w_1, \\ [u, x_2] &= x_1, \quad [c, y] = a, \quad [d, y_2] = b, \quad [d, u] = c, \quad [y_2, u] = y, \\ [x_1, y_2] &= tz, \quad [w_1, y_2] = [a, x_2] = [b, y] = vz, \\ [w, y_2] &= [w_1, y] = [b, x_2] = [a, b] = vt, \quad [d, x_2] = wv, \\ [x_2, y_2] &= vtz, \quad [c, x_2] = w_1wtz, \quad [b, u] = ax_1wv, \\ [d, y] &= abx_2vt, \quad [c, y_2] = abx_1x_2w_1. \end{aligned}$$

Das Abzählen der Nebenklassen von  $\langle a, b, y \rangle$  in  $S$  mit Hilfe des in MAGMA [2] implementierten Todd-Coxeter-Algorithmus liefert eine treue Permutationsdarstellung  $\pi_S : S \hookrightarrow \mathbf{S}_{512}$ . Ohne Einschränkung dürfen wir daher fortan  $S$  mit  $\pi_S(S)$  identifizieren.

Als maximaler 2-Normalteiler des gesuchten Zentralisators  $H$  sollte sich die in Lemma 5.1.2 beschriebene Gruppe  $J$  auch in unserer konkreten Instanz der 2-Sylowuntergruppe  $S$  von  $H$  wieder finden. Und tatsächlich haben wir keine allzu große Auswahl.

**Lemma 5.1.4**

Es sei  $S$  die in Satz 5.1.3 presentierete Gruppe. Dann gelten:

(a) Die Untergruppe

$$J := \langle z, t, v, w, w_1, x_1, x_2, a, b, c, d \rangle \leq S$$

ist der einzige Normalteiler von  $S$  der Ordnung  $|J| = 2^{11}$  mit einem zyklischen Zentrum  $\mathbf{Z}(J) = \langle z \rangle$  und Nilpotenzklasse  $c(J) = 3$ .

(b) Die Untergruppen

$$A := \langle z, t, v, w, a \rangle \leq J \quad \text{und} \quad B := \langle z, t, v, w, w_1 \rangle \leq J$$

sind in  $S$  die elementar abelschen Normalteiler maximaler Ordnung  $|A| = |B| = 2^5$ ; ferner ist  $A = \mathbf{C}_J(A) = \mathbf{C}_S(A)$ , wohingegen  $B < \mathbf{C}_J(B) = \mathbf{C}_S(B) = \langle B, x_1, x_2 \rangle$ .

(c)  $B = J' = \Phi(J)$  und  $\mathbf{Z}(J) = [J, J']$ ;

(d)  $J$  besitzt in  $S$  genau zwei konjugierten Klassen von Komplementen. Representanten dieser Klassen sind

$$K_1 := \langle y, y_2, u \rangle \quad \text{bzw.} \quad K_2 := \langle y, y_2, zu \rangle,$$

beide isomorph zur Diedergruppe  $D_8$ .

**Beweis.** Eine Diskussion des Normalteilerverbandes von  $S$  unter MAGMA bestatigt uns die Behauptungen (a) und (b). Auch die Gleichungen in (c) verifiziert das Programm sofort.

Um den ersten Teil von (d) einzusehen, mussen die 2-Gruppen  $S$  und  $J$  vorubergehend als polyzyklische Gruppen dargestellt werden, weil die das Problem losende MAGMA-Funktion `Complements` lediglich auf Argumente aus der Kategorie `GrpPC` anwendbar ist. Die Isomorphiebeziehungen  $K_1 \cong D_8 \cong K_2$  folgen indes schon aus der Tatsache, dass die Teilmenge

$$\mathcal{D} := \{ y^2 = y_2^2 = u^2 = 1, [y, y_2] = [y, u] = 1, [y_2, u] = y \}$$

der in Satz 5.1.3 angegebenen Relationenmenge  $\mathcal{S}$  eine definierende Relationenmenge fur die Diedergruppe  $D_8$  ist.  $\square$

Innerhalb des zu konstruierenden Zentralisators  $H$  hat wegen Lemma 5.1.4(b) offensichtlich nur der elementar abelsche Normalteiler  $B$  von  $S$  eine Chance, die Rolle der Gruppe  $E$  aus Lemma 5.1.2 ubernehmen zu konnen. Dass sich  $Q := \langle x_1, x_2 \rangle$  bei genauerem Hinsehen als Quaternionengruppe der Ordnung 8 mit Zentrum  $\mathbf{Z}(Q) = \langle z \rangle$  herausstellt, untermauert diesen Schluss zusatzlich, denn damit haben wir wie vorausgesagt  $\mathbf{C}_J(B) = \langle t, v, w, w_1, Q \rangle \cong 2^4 \times Q_8$ .

Gemaß Bedingung (ii) aus Satz 5.1.1 besteht unsere Aufgabe jetzt darin, ein Komplement von  $J$  in  $S$  in eine symmetrische Gruppe  $S_5$  einzubetten und diese sodann in wohldefinierter Art und Weise auf dem Normalteiler  $J$  zum Operieren zu bringen. Ohne Beschrankung der Allgemeinheit durfen wir uns dabei auf das Komplement  $K := K_1$  kaprizieren, da  $z \in \mathbf{Z}(S)$  gilt und die Konjugationsaktion des Erzeugers  $zu$  von  $K_2$  auf  $J$  deshalb exakt mit der des Erzeugers  $u$  von  $K_1$  ubereinstimmt.

Erleichternd kommt hinzu, dass es sich bei  $D_8$  gerade um die Struktur einer 2-Sylowuntergruppe von  $S_5$  handelt. Nach dem Satz von Sylow sind folglich je zwei mögliche Bilder von  $K$  zueinander konjugiert.

**Lemma 5.1.5**

Mit der im Beweis von Lemma 5.1.4 eingeführten Relationenmenge  $\mathcal{D}$  gilt:

$$P := \langle y, y_2, u, f \mid \mathcal{D}, f^5 = 1, y^f = yy_2fy_2f, y_2^f = yfy_2, u^f = yufy_2f^2 \rangle$$

ist eine endliche Präsentation der symmetrischen Gruppe  $S_5$ .

**Beweis.** Mit Hilfe von MAGMA rechnet man nach, dass die Relationenmenge von  $P$  eine bis auf Isomorphie eindeutige Gruppe der Ordnung 120 definiert und dass vermöge

$$y \mapsto (1, 2)(3, 4), \quad y_2 \mapsto (1, 3)(2, 4), \quad u \mapsto (1, 2), \quad f \mapsto (1, 2, 3, 4, 5)$$

ein Isomorphismus von  $P$  auf die natürliche Permutationsdarstellung der symmetrischen Gruppe  $S_5$  induziert wird.  $\square$

Nun bleibt zu klären, ob sich diese spezielle Operation eines neuen Erzeugers  $f$  der Ordnung 5 wirklich auf die volle 2-Sylowuntergruppe  $S$  erweitern lässt. Gesucht sind also Relationen, welche die Konjugationsaktion von  $f$  auf den Erzeugern von  $J$  regeln, um die Vereinigung der Präsentationen von  $S$  und  $P$  schließlich zu einer endlichen Präsentation von  $H$  auszubauen.

Die kanonische Operation des Komplements  $K$  auf einer elementar abelschen Faktorgruppe von  $J$  der Ordnung  $2^n$  kann durch einen Monomorphismus  $\varphi : K \rightarrow \text{GL}_n(2)$  beschrieben werden. Indem wir erörtern, wie  $\varphi$  auf ganz  $P$  fortgesetzt werden kann, erhalten wir zugleich auch ein ausschnittsweises Bild von allen zulässigen Aktionen, die für  $f$  auf  $J$  in Betracht zu ziehen sind.

**Lemma 5.1.6**

Mit den in Lemma 5.1.4 eingeführten Bezeichnungen gilt:

- (a) Die Faktorgruppe  $\bar{J} := J/\mathbf{C}_J(B)$  ist elementar abelsch der Ordnung  $2^4$  und wird erzeugt von den Linksnebenklassen  $\bar{a}, \bar{b}, \bar{c}$  und  $\bar{d}$ , wobei  $\bar{g} := g\mathbf{C}_J(B)$  für  $g \in J$ .
- (b) Die Faktorgruppe  $\hat{J} := J/B$  ist elementar abelsch der Ordnung  $2^6$  und wird erzeugt von den Linksnebenklassen  $\hat{x}_1, \hat{x}_2, \hat{a}, \hat{b}, \hat{c}$  und  $\hat{d}$ , wobei  $\hat{g} := gB$  für  $g \in J$ .

**Beweis.** Aus der Präsentation von  $S$  in Satz 5.1.3 liest man mit einem Seitenblick auf Lemma 5.1.4(a), (b) ab, dass  $\bar{J}$  und  $\hat{J}$  elementar abelsche Gruppen der Ordnung  $2^4$  bzw.  $2^6$  sind. Außerdem liegt  $S$  unter MAGMA als Permutationsgruppe vor, weshalb die Frage, ob zwei gegebene Elemente unterschiedliche Linksnebenklassen von  $\mathbf{C}_J(B)$  bzw.  $B$  repräsentieren, mühelos per Rechner beantwortet werden kann.  $\square$

Interpretieren wir  $\bar{J}$  als vierdimensionalen Vektorraum über dem Körper  $\text{GF}(2)$ , so ergibt sich bezüglich der geordneten Basis  $(\bar{a}, \bar{b}, \bar{c}, \bar{d})$  von  $\bar{J}$  folgender Monomorphismus  $\bar{\varphi} : K \rightarrow \text{GL}_4(2)$ :

$$\bar{\varphi}(y) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \quad \text{denn } a^y = a, \quad b^y = bvz, \quad c^y = ca \quad \text{und} \quad d^y = dabbx_2vt;$$

$$\bar{\varphi}(y_2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad \text{denn } a^{y_2} = at, \ b^{y_2} = b, \ c^{y_2} = cabx_1x_2w_1 \text{ und } d^{y_2} = db;$$

$$\bar{\varphi}(u) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \text{denn } a^u = a, \ b^u = bax_1wv, \ c^u = c \text{ und } d^u = dc.$$

Die Gruppe  $\text{GL}_4(2)$  besitzt genau eine Konjugiertenklasse von Elementen der Ordnung 5. MAGMA findet in dieser Klasse lediglich vier Matrizen, die auf  $\bar{\varphi}(y)$ ,  $\bar{\varphi}(y_2)$  bzw.  $\bar{\varphi}(u)$  in derselben Weise wirken wie  $f \in P$  auf  $y$ ,  $y_2$  bzw.  $u$ :

$$F_1 := \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad F'_1 := \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad F_2 := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad F'_2 := \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix},$$

wobei  $S_5 \cong \langle \bar{\varphi}(K), F_1 \rangle = \langle \bar{\varphi}(K), F'_1 \rangle \leq \text{GL}_4(2)$  und  $S_5 \cong \langle \bar{\varphi}(K), F_2 \rangle = \langle \bar{\varphi}(K), F'_2 \rangle \leq \text{GL}_4(2)$ .

Analog induziert bereits die Konjugationsoperation von  $K$  auf  $B$  bezüglich der geordneten Basis  $(z, t, v, w, w_1)$  einen Monomorphismus  $\varphi : K \rightarrow \text{GL}_5(2)$  mit

$$\varphi(y) = \left( \begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & & \\ 0 & & & \end{array} \begin{array}{c} \varphi(y) \end{array} \right), \quad \varphi(y_2) = \left( \begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ 0 & & & \\ 0 & & & \\ 1 & & & \end{array} \begin{array}{c} \varphi(y_2) \end{array} \right), \quad \varphi(u) = \left( \begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & & \\ 0 & & & \end{array} \begin{array}{c} \varphi(u) \end{array} \right).$$

Insbesondere erkennen wir, dass  $\bar{J}$  und  $B/\langle z \rangle$  als  $K$ -Moduln über  $\text{GF}(2)$  isomorph sind.

Auch in  $\text{GL}_5(2)$  existiert genau eine Konjugiertenklasse von Elementen der Ordnung 5 und wiederum findet MAGMA darin im Wesentlichen vier Matrizen, die auf  $\varphi(y)$ ,  $\varphi(y_2)$  bzw.  $\varphi(u)$  in derselben Weise wirken wie  $f \in P$  auf  $y$ ,  $y_2$  bzw.  $u$ , nämlich

$$F_{11} = \left( \begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 1 & & & \\ 0 & & & \\ 1 & & & \\ 0 & & & \end{array} \begin{array}{c} F_1 \end{array} \right), \quad F_{12} = \left( \begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ 1 & & & \\ 1 & & & \\ 0 & & & \end{array} \begin{array}{c} F_1 \end{array} \right),$$

$$F_{21} = \left( \begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ 1 & & & \\ 1 & & & \\ 0 & & & \end{array} \begin{array}{c} F_2 \end{array} \right) \quad \text{und} \quad F_{22} = \left( \begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 1 & & & \\ 0 & & & \\ 1 & & & \\ 1 & & & \end{array} \begin{array}{c} F_2 \end{array} \right).$$

Zu jeder Matrix  $F_{ij}$ ,  $i, j \in \{1, 2\}$ , enthält die  $S_5$ -Untergruppe  $\langle \varphi(K), F_{ij} \rangle \leq \text{GL}_5(2)$  noch eine weitere „Lösung“ mit  $F'_i$  als rechtem unteren  $4 \times 4$ -Block.

Prinzipiell liefern die Matrizen  $F_{ij}$  sofort all jene Pakete von Relationen, welche theoretisch mögliche Konjugationsaktionen von  $f$  auf  $B$  zum Ausdruck bringen. Weil jedoch  $B = J'$  gilt,

benötigen wir solche Relationen gar nicht; aus der Formel  $[g, h]^x = [g^x, h^x]$  geht die Operation von  $f$  auf  $B$  eindeutig hervor, sobald bekannt ist wie  $f$  auf  $x_1, x_2, a, b, c$  und  $d$  agiert. Nichtsdestoweniger lohnt sich die Analyse der zumindest hinsichtlich ihrer Präsentation verschiedenen Erweiterungen  $B:P$ , da sie uns in die Lage versetzt, die Konjugationsaktion von  $f$  auf  $x_1$  und  $x_2$  separat, das heißt entkoppelt von der auf  $\hat{J}$  zu ermitteln.

**Lemma 5.1.7**

Unter Verwendung der bisher eingeführten Bezeichnungen gehorcht die Operation von  $f$  auf der Quaternionengruppe  $Q = \langle x_1, x_2 \rangle$  Relationen der Form

$$x_1^f = x_1 z^{\varepsilon_1} t^{\varepsilon_2} v^{\varepsilon_3} w^{\varepsilon_4} w_1^{\varepsilon_5} \quad \text{bzw.} \quad x_2^f = x_2 z^{\nu_1} t^{\nu_2} v^{\nu_3} w^{\nu_4} w_1^{\nu_5}$$

mit Exponentenvektoren  $\varepsilon := (\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5), \nu := (\nu_1, \nu_2, \nu_3, \nu_4, \nu_5) \in \{0, 1\}^5$ .

**Beweis.** Für eine 5-Sylowuntergruppe  $R$  des zu konstruierenden Zentralisators  $H$  gilt laut Parrot [35], Lemma 3:  $\mathbf{C}_J(R) = \mathbf{C}_{\mathbf{C}_J(B)}(R) \cong \mathbf{Q}_8$ . Aufgrund der  $(2^4 \times \mathbf{Q}_8)$ -Struktur von  $\mathbf{C}_J(B)$  folgt daraus  $\mathbf{C}_{\hat{J}}(R) = \langle \hat{x}_1, \hat{x}_2 \rangle$  und wegen Bedingung (ii) in Satz 5.1.1 muss  $R$  zyklisch der Ordnung 5 sein. Modulo  $B$  vertauscht der Erzeuger  $f$  demnach sowohl mit  $x_1$  als auch mit  $x_2$ .  $\square$

Aus dem für  $\mathbf{C}_J(B)$  relevanten Teil der Präsentation von  $S$ , der Präsentation von  $P$ , den aus jeweils einer der Matrizen  $F_{ij}$ ,  $i, j \in \{1, 2\}$ , abgeleiteten Relationen sowie den generischen Relationen gemäß Lemma 5.1.7 lassen sich jetzt  $2^{5 \cdot 2}$  durch die Exponentenvektoren  $\varepsilon$  und  $\nu$  parametrisierte endliche Präsentationen bauen. Mit Hilfe der MAGMA-Implementierung des Todd-Coxeter-Algorithmus verifiziert man schnell, dass nur 16 der korrespondierenden Gruppen die für eine Erweiterung  $\mathbf{C}_J(B) : S_5$  zu erwartende Ordnung  $2^{10} \cdot 3 \cdot 5 = 15360$  aufweisen:

$f$ -Matrix	„zulässige“ Exponentenvektorenpaare $\varepsilon = \dots$ $\nu = \dots$			
$F_{11}$	$(0, 0, 0, 1, 0)$	$(\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0})$	$(1, 1, 1, 0, 1)$	$(1, 1, 1, 0, 1)$
	$(0, 0, 1, 1, 0)$	$(\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1})$	$(1, 1, 1, 0, 0)$	$(0, 0, 0, 1, 1)$
$F_{12}$	$(0, 0, 0, 1, 0)$	$(0, 0, 0, 1, 0)$	$(\mathbf{0}, \mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{1})$	$(0, 1, 1, 0, 1)$
	$(0, 0, 1, 1, 0)$	$(0, 1, 0, 0, 1)$	$(\mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0})$	$(1, 0, 0, 1, 1)$
$F_{21}$	$(0, 0, 0, 1, 0)$	$(0, 0, 0, 1, 0)$	$(0, 0, 1, 0, 1)$	$(0, 0, 1, 0, 1)$
	$(0, 0, 1, 1, 0)$	$(0, 0, 0, 0, 1)$	$(1, 1, 1, 0, 0)$	$(1, 1, 0, 1, 1)$
$F_{22}$	$(0, 0, 0, 1, 0)$	$(0, 0, 0, 1, 0)$	$(1, 0, 1, 0, 1)$	$(1, 0, 1, 0, 1)$
	$(0, 0, 1, 1, 0)$	$(1, 0, 0, 0, 1)$	$(1, 1, 1, 0, 0)$	$(0, 1, 0, 1, 1)$

Betrachten wir nun die kanonische Operation von  $K$  auf der Faktorgruppe  $\hat{J}$ , interpretiert als sechsdimensionaler Vektorraum über dem Körper  $\text{GF}(2)$ . Bezüglich der geordneten Basis  $(\hat{x}_1, \hat{x}_2, \hat{a}, \hat{b}, \hat{c}, \hat{d})$  von  $\hat{J}$  ergibt sich ein Monomorphismus  $\hat{\varphi} : K \rightarrow \text{GL}_6(2)$  mit

$$\hat{\varphi}(y) = \left( \begin{array}{cc|ccc} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & & & \\ 0 & 0 & & & \\ 0 & 0 & \hat{\varphi}(y) & & \\ 0 & 1 & & & \end{array} \right), \quad \text{denn } x_1^y = x_1 \text{ und } x_2^y = x_2 z;$$



$$\hat{\varphi}(y_2) = \left( \begin{array}{cc|ccc} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & & & \\ 0 & 0 & & & \\ 1 & 1 & \bar{\varphi}(y_2) & & \\ 0 & 0 & & & \end{array} \right), \quad \text{denn } x_1^{y_2} = x_1 t z \text{ und } x_2^{y_2} = x_2 v t z;$$

$$\hat{\varphi}(u) = \left( \begin{array}{cc|ccc} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & & & \\ 1 & 0 & & & \\ 0 & 0 & \bar{\varphi}(u) & & \\ 0 & 0 & & & \end{array} \right), \quad \text{denn } x_1^u = x_1 z, \ x_2^u = x_2 x_1^{-1} \text{ und } \hat{x}_1^2 = 1.$$

Bei der Suche nach Elementen der Ordnung 5 von  $\text{GL}_6(2)$ , die auf  $\hat{\varphi}(y)$ ,  $\hat{\varphi}(y_2)$  bzw.  $\hat{\varphi}(u)$  in exakt derselben Weise wirken wie  $f \in P$  auf  $y$ ,  $y_2$  bzw.  $u$  dürfen wir uns angesichts der vier potentiellen Fortsetzungen von  $\bar{\varphi}$  auf  $P$  und Lemma 5.1.7 auf

$$\left\{ \left( \frac{I_2}{*} \middle| \frac{\mathbf{0}}{F} \right) \middle| F \in \{F_1, F'_1, F_2, F'_2\} \right\} \subseteq \text{GL}_6(2)$$

als Kandidatenmenge beschränken. Aus jeder gefundenen „Lösungsmatrix“ ergibt sich ein Satz von Relationen, welcher modulo  $B$  eine mögliche Operation von  $f$  auf  $J$  beschreibt. Um daraus tunlichst effizient Rückschlüsse auf die tatsächlichen, sprich in  $H$  gültigen Relationen ziehen zu können, fehlt uns noch ein geeignetes Werkzeug.

#### Lemma 5.1.8

*Unter Verwendung der bisher eingeführten Bezeichnungen gilt:*

*Für  $g \in \{a, b, c, d\}$  und ein Wort  $r = r(x_1, x_2, a, b, c, d)$  in den Linksnebenklassenvertretern von  $B$  in  $J$  folgt aus der Relation  $\hat{g}^f = \hat{r}$  die Existenz eines Elements  $e \in B$  mit  $g^f = r \cdot e$ , wobei*

$$e \in \mathbf{C}_B(r) \iff r^2 = 1.$$

**Beweis.** Die Existenz eines  $e \in B$  mit der behaupteten Eigenschaft ist trivial. Zu zeigen ist daher lediglich die Äquivalenzaussage.

Weil  $e$  als Element einer elementar abelschen 2-Gruppe sein eigenes Inverses ist, gilt einerseits  $r^2 = r^2 e^2$ . Da jede Konjugation die Elementordnung respektiert, haben wir andererseits  $(re)^2 = g^2 = 1$ . Beide Gleichungen dürfen genau dann zu einer Kette verbunden werden, wenn  $r^2 e^2 = (re)^2$  bzw.  $re = er$ .  $\square$

Damit treten wir in die für diesen Abschnitt wesentliche Fallunterscheidung ein.

**Fall 1:** Sei  $F := F_1$ . MAGMA findet genau vier  $4 \times 2$ -Blöcke  $X$ , so dass

$$\mathfrak{F}_1(X) := \left( \frac{I_2}{X} \middle| \frac{\mathbf{0}}{F} \right) \in \text{GL}_6(2)$$

eine Matrix der Ordnung 5 ist, die per Konjugation auf  $\hat{\varphi}(y)$ ,  $\hat{\varphi}(y_2)$  bzw.  $\hat{\varphi}(u)$  in exakt derselben Weise agiert wie  $f \in P$  auf  $y$ ,  $y_2$  bzw.  $u$ , nämlich

$$X_{11} := \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad X_{12} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad X_{13} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad X_{14} := \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Die vier Untergruppen  $\langle \hat{\varphi}(K), \mathfrak{F}_1(X_{1i}) \rangle \leq \text{GL}_6(2)$ ,  $i = 1, 2, 3, 4$ , sind vier verschiedene, in  $\mathbf{C}_{\text{GL}_6(2)}(\hat{\varphi}(K))$  paarweise konjugierte Kopien der symmetrischen Gruppe  $S_5$  — und zwar genau dieselben, welche sich analog für die Wahl  $F = F'_1$  ergeben. Die Betrachtung dieses letzteren Falles ist mithin überflüssig.

**Fall 1.1:**

Sei  $\hat{\varphi}(f) := \mathfrak{F}_1(X_{11})$ , also  $\hat{a}^f = \hat{x}_2 \hat{b} \hat{c} \hat{d}$ ,  $\hat{b}^f = \hat{d}$ ,  $\hat{c}^f = \hat{x}_1 \hat{a} \hat{b}$  und  $\hat{d}^f = \hat{c} \hat{d}$ .

Mit Hilfe von MAGMA rechnet man nach, dass

(1)  $\text{ord}(x_2 bcd) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$a^f = x_2 bcd \cdot e_a$$

für ein  $e_a \in B \setminus \mathbf{C}_B(x_2 bcd) = B \setminus \langle z, tv, vw, w_1 \rangle$ .

Mit Exponentenvektor  $\alpha \in \{0, 1\}^4$  ist der Faktor  $e_a$  deshalb von der Form

$$e_a = z^{\alpha_1} t^{\alpha_2} v^{\alpha_3} w^{\alpha_2 + \alpha_3 + 1} w_1^{\alpha_4}.$$

(2)  $\text{ord}(d) = 2$ ; laut Lemma 5.1.8 gilt

$$b^f = d \cdot e_b$$

für ein  $e_b \in \mathbf{C}_B(d) = \langle z, v, w, w_1 \rangle$ .

Mit Exponentenvektor  $\beta \in \{0, 1\}^4$  ist der Faktor  $e_b$  deshalb von der Form

$$e_b = z^{\beta_1} v^{\beta_2} w^{\beta_3} w_1^{\beta_4}.$$

(3)  $\text{ord}(x_1 ab) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$c^f = x_1 ab \cdot e_c$$

für ein  $e_c \in B \setminus \mathbf{C}_B(x_1 ab) = B \setminus \langle z, t, v, ww_1 \rangle$ .

Mit Exponentenvektor  $\gamma \in \{0, 1\}^4$  ist der Faktor  $e_c$  deshalb von der Form

$$e_c = z^{\gamma_1} t^{\gamma_2} v^{\gamma_3} w^{\gamma_4} w_1^{\gamma_4 + 1}.$$

(4)  $\text{ord}(cd) = 2$ ; laut Lemma 5.1.8 gilt

$$d^f = cd \cdot e_d$$

für ein  $e_d \in \mathbf{C}_B(cd) = \langle z, tv, w, w_1 \rangle$ .

Mit Exponentenvektor  $\delta \in \{0, 1\}^4$  ist der Faktor  $e_d$  deshalb von der Form

$$e_d = z^{\delta_1} (tv)^{\delta_2} w^{\delta_3} w_1^{\delta_4}.$$

**Fall 1.2:**

Sei  $\hat{\varphi}(f) := \mathfrak{F}_1(X_{12})$ , also  $\hat{a}^f = \hat{x}_1 \hat{x}_2 \hat{b} \hat{c} \hat{d}$ ,  $\hat{b}^f = \hat{x}_1 \hat{d}$ ,  $\hat{c}^f = \hat{x}_1 \hat{a} \hat{b}$  und  $\hat{d}^f = \hat{c} \hat{d}$ .

Mit Hilfe von MAGMA rechnet man nach, dass

(1)  $\text{ord}(x_1 x_2 bcd) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$a^f = x_1 x_2 bcd \cdot e_a$$

für ein  $e_a \in B \setminus \mathbf{C}_B(x_1 x_2 bcd) = B \setminus \langle z, tv, vw, w_1 \rangle$ .

Deshalb ist der Faktor  $e_a$  von der gleichen Form wie in Fall 1.1.

(2)  $\text{ord}(x_1d) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$b^f = x_1d \cdot e_b$$

für ein  $e_b \in B \setminus \mathbf{C}_B(x_1d) = B \setminus \langle z, v, w, w_1 \rangle$ .

Mit Exponentenvektor  $\beta \in \{0, 1\}^4$  ist der Faktor  $e_b$  deshalb von der Form

$$e_b = z^{\beta_1} t v^{\beta_2} w^{\beta_3} w_1^{\beta_4}.$$

(3), (4) identisch zu Fall 1.1.

**Fall 1.3:**

Sei  $\hat{\varphi}(f) := \mathfrak{F}_1(X_{13})$ , also  $\hat{a}^f = \hat{x}_1 \hat{b} \hat{c} \hat{d}$ ,  $\hat{b}^f = \hat{x}_2 \hat{d}$ ,  $\hat{c}^f = \hat{a} \hat{b}$  und  $\hat{d}^f = \hat{x}_1 \hat{c} \hat{d}$ .

Mit Hilfe von MAGMA rechnet man nach, dass

(1)  $\text{ord}(x_1bcd) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$a^f = x_1bcd \cdot e_a$$

für ein  $e_a \in B \setminus \mathbf{C}_B(x_1bcd) = B \setminus \langle z, tv, vw, w_1 \rangle$ .

Deshalb ist der Faktor  $e_a$  von der gleichen Form wie in Fall 1.1.

(2)  $\text{ord}(x_2d) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$b^f = x_2d \cdot e_b$$

für ein  $e_b \in B \setminus \mathbf{C}_B(x_2d) = B \setminus \langle z, v, w, w_1 \rangle$ .

Deshalb ist der Faktor  $e_b$  von der gleichen Form wie in Fall 1.2.

(3)  $\text{ord}(ab) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$c^f = ab \cdot e_c$$

für ein  $e_c \in B \setminus \mathbf{C}_B(ab) = B \setminus \langle z, t, v, ww_1 \rangle$ .

Deshalb ist der Faktor  $e_c$  von der gleichen Form wie in Fall 1.1.

(4)  $\text{ord}(x_1cd) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$d^f = x_1cd \cdot e_d$$

für ein  $e_d \in B \setminus \mathbf{C}_B(x_1cd) = B \setminus \langle z, tv, w, w_1 \rangle$ .

Mit Exponentenvektor  $\delta \in \{0, 1\}^4$  ist der Faktor  $e_d$  deshalb von der Form

$$e_d = z^{\delta_1} t^{\delta_2} v^{\delta_2+1} w^{\delta_3} w_1^{\delta_4}.$$

**Fall 1.4:**

Sei  $\hat{\varphi}(f) := \mathfrak{F}_1(X_{14})$ , also  $\hat{a}^f = \hat{b} \hat{c} \hat{d}$ ,  $\hat{b}^f = \hat{x}_1 \hat{x}_2 \hat{d}$ ,  $\hat{c}^f = \hat{a} \hat{b}$  und  $\hat{d}^f = \hat{x}_1 \hat{c} \hat{d}$ .

Mit Hilfe von MAGMA rechnet man nach, dass

(1)  $\text{ord}(bcd) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$a^f = bcd \cdot e_a$$

für ein  $e_a \in B \setminus \mathbf{C}_B(bcd) = B \setminus \langle z, tv, vw, w_1 \rangle$ .

Deshalb ist der Faktor  $e_a$  von der gleichen Form wie in Fall 1.1.

(2)  $\text{ord}(x_1x_2d) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$b^f = x_1x_2d \cdot e_b$$

für ein  $e_b \in B \setminus \mathbf{C}_B(x_1x_2d) = B \setminus \langle z, v, w, w_1 \rangle$ .

Deshalb ist der Faktor  $e_b$  von der gleichen Form wie in Fall 1.2.

(3), (4) identisch zu Fall 1.3.

**Fall 2:** Sei  $F := F_2$ . MAGMA findet genau vier  $4 \times 2$ -Blöcke  $X$ , so dass

$$\mathfrak{F}_2(X) := \left( \frac{I_2}{X} \middle| \frac{\mathbf{0}}{F} \right) \in \text{GL}_6(2)$$

eine Matrix der Ordnung 5 ist, die per Konjugation auf  $\hat{\varphi}(y)$ ,  $\hat{\varphi}(y_2)$  bzw.  $\hat{\varphi}(u)$  in exakt derselben Weise agiert wie  $f \in P$  auf  $y$ ,  $y_2$  bzw.  $u$ , nämlich

$$X_{21} := \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad X_{22} := \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X_{23} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{und} \quad X_{24} := X_{14}.$$

Die vier Untergruppen  $\langle \hat{\varphi}(K), \mathfrak{F}_2(X_{2i}) \rangle \leq \text{GL}_6(2)$ ,  $i = 1, 2, 3, 4$ , sind vier verschiedene, in  $\mathbf{C}_{\text{GL}_6(2)}(\hat{\varphi}(K))$  paarweise konjugierte Kopien der symmetrischen Gruppe  $S_5$  — und zwar genau dieselben, welche sich analog für die Wahl  $F = F'_2$  ergeben. Die Betrachtung dieses letzteren Falles ist mithin überflüssig.

**Fall 2.1:**

Sei  $\hat{\varphi}(f) := \mathfrak{F}_2(X_{21})$ , also  $\hat{a}^f = \hat{x}_1\hat{x}_2\hat{a}\hat{b}\hat{c}\hat{d}$ ,  $\hat{b}^f = \hat{x}_1\hat{a}\hat{d}$ ,  $\hat{c}^f = \hat{x}_1\hat{a}\hat{b}$  und  $\hat{d}^f = \hat{x}_1\hat{x}_2\hat{b}$ .

Mit Hilfe von MAGMA rechnet man nach, dass

(1)  $\text{ord}(x_1x_2abcd) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$a^f = x_1x_2abcd \cdot e_a$$

für ein  $e_a \in B \setminus \mathbf{C}_B(x_1x_2abcd) = B \setminus \langle z, tv, vw, ww_1 \rangle$ .

Mit Exponentenvektor  $\alpha \in \{0, 1\}^4$  ist der Faktor  $e_a$  deshalb von der Form

$$e_a = z^{\alpha_1} t^{\alpha_2} v^{\alpha_3} w^{\alpha_4} w_1^{\alpha_2 + \alpha_3 + \alpha_4 + 1}.$$

(2)  $\text{ord}(x_1ad) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$b^f = x_1ad \cdot e_b$$

für ein  $e_b \in B \setminus \mathbf{C}_B(x_1ad) = \langle z, tw_1, v, w \rangle$ .

Mit Exponentenvektor  $\beta \in \{0, 1\}^4$  ist der Faktor  $e_b$  deshalb von der Form

$$e_b = z^{\beta_1} t^{\beta_2} v^{\beta_3} w^{\beta_4} w_1^{\beta_2 + 1}.$$

(3) identisch zu Fall 1.1.

- (4)  $\text{ord}(x_1x_2b) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$d^f = x_1x_2b \cdot e_d$$

für ein  $e_d \in B \setminus \mathbf{C}_B(x_1x_2b) = \langle z, t, v, w_1 \rangle$ .

Mit Exponentenvektor  $\delta \in \{0, 1\}^4$  ist der Faktor  $e_d$  deshalb von der Form

$$e_d = z^{\delta_1} t^{\delta_2} v^{\delta_3} w w_1^{\delta_4}.$$

**Fall 2.2:**

Sei  $\hat{\varphi}(f) := \mathfrak{F}_2(X_{22})$ , also  $\hat{a}^f = \hat{x}_2 \hat{a} \hat{b} \hat{c} \hat{d}$ ,  $\hat{b}^f = \hat{a} \hat{d}$ ,  $\hat{c}^f = \hat{x}_1 \hat{a} \hat{b}$  und  $\hat{d}^f = \hat{x}_2 \hat{b}$ .

Mit Hilfe von MAGMA rechnet man nach, dass

- (1)  $\text{ord}(x_2abcd) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$a^f = x_2abcd \cdot e_a$$

für ein  $e_a \in B \setminus \mathbf{C}_B(x_2abcd) = B \setminus \langle z, tv, vw, ww_1 \rangle$ .

Deshalb ist der Faktor  $e_a$  von der gleichen Form wie in Fall 2.1.

- (2)  $\text{ord}(ad) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$b^f = ad \cdot e_b$$

für ein  $e_b \in B \setminus \mathbf{C}_B(ad) = \langle z, tw_1, v, w \rangle$ .

Deshalb ist der Faktor  $e_b$  von der gleichen Form wie in Fall 2.1.

- (3) identisch zu Fall 1.1.

- (4)  $\text{ord}(x_2b) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$d^f = x_2b \cdot e_d$$

für ein  $e_d \in B \setminus \mathbf{C}_B(x_2b) = \langle z, t, v, w_1 \rangle$ .

Deshalb ist der Faktor  $e_d$  von der gleichen Form wie in Fall 2.1.

**Fall 2.3:**

Sei  $\hat{\varphi}(f) := \mathfrak{F}_2(X_{23})$ , also  $\hat{a}^f = \hat{x}_1 \hat{a} \hat{b} \hat{c} \hat{d}$ ,  $\hat{b}^f = \hat{x}_2 \hat{a} \hat{d}$ ,  $\hat{c}^f = \hat{a} \hat{b}$  und  $\hat{d}^f = \hat{b}$ .

Mit Hilfe von MAGMA rechnet man nach, dass

- (1)  $\text{ord}(x_1abcd) = 2$ ; laut Lemma 5.1.8 gilt

$$a^f = x_1abcd \cdot e_a$$

für ein  $e_a \in \mathbf{C}_B(x_1abcd) = \langle z, tv, vw, ww_1 \rangle$ .

Mit Exponentenvektor  $\alpha \in \{0, 1\}^4$  ist der Faktor  $e_a$  deshalb von der Form

$$e_a = z^{\alpha_1} t^{\alpha_2} v^{\alpha_3} w^{\alpha_4} w_1^{\alpha_2 + \alpha_3 + \alpha_4}.$$

- (2)  $\text{ord}(x_2ad) = 2$ ; laut Lemma 5.1.8 gilt

$$b^f = x_2ad \cdot e_b$$

für ein  $e_b \in \mathbf{C}_B(x_2ad) = \langle z, tw_1, v, w \rangle$ .

Mit Exponentenvektor  $\beta \in \{0, 1\}^4$  ist der Faktor  $e_b$  deshalb von der Form

$$e_b = z^{\beta_1} t^{\beta_2} v^{\beta_3} w^{\beta_4} w_1^{\beta_2}.$$

- (3) identisch zu Fall 1.3.  
 (4)  $\text{ord}(b) = 2$ ; laut Lemma 5.1.8 gilt

$$d^f = b \cdot e_d$$

für ein  $e_d \in \mathbf{C}_B(b) = \langle z, t, v, w_1 \rangle$ .

Mit Exponentenvektor  $\delta \in \{0, 1\}^4$  ist der Faktor  $e_d$  deshalb von der Form

$$e_d = z^{\delta_1} t^{\delta_2} v^{\delta_3} w_1^{\delta_4}.$$

**Fall 2.4:**

Sei  $\hat{\varphi}(f) := \mathfrak{F}_2(X_{24})$ , also  $\hat{a}^f = \hat{a}\hat{b}\hat{c}\hat{d}$ ,  $\hat{b}^f = \hat{x}_1\hat{x}_2\hat{a}\hat{d}$ ,  $\hat{c}^f = \hat{a}\hat{b}$  und  $\hat{d}^f = \hat{x}_1\hat{b}$ .

Mit Hilfe von MAGMA rechnet man nach, dass

- (1)  $\text{ord}(abcd) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$a^f = abcd \cdot e_a$$

für ein  $e_a \in B \setminus \mathbf{C}_B(abcd) = B \setminus \langle z, tv, vw, ww_1 \rangle$ .

Deshalb ist der Faktor  $e_a$  von der gleichen Form wie in Fall 2.1.

- (2)  $\text{ord}(x_1x_2ad) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$b^f = x_1x_2ad \cdot e_b$$

für ein  $e_b \in B \setminus \mathbf{C}_B(x_1x_2ad) = B \setminus \langle z, tw_1, v, w \rangle$ .

Deshalb ist der Faktor  $e_b$  von der gleichen Form wie in Fall 2.1.

- (3) identisch zu Fall 1.3.  
 (4)  $\text{ord}(x_1b) = 4 \neq 2$ ; laut Lemma 5.1.8 gilt

$$d^f = x_1b \cdot e_d$$

für ein  $e_d \in B \setminus \mathbf{C}_B(x_1b) = B \setminus \langle z, t, v, w_1 \rangle$ .

Deshalb ist der Faktor  $e_d$  von der gleichen Form wie in Fall 2.1.

Aus den Präsentationen von  $S$  und  $P$ , den über die  $2 \cdot 2^3$  Exponentenvektorraare  $(\varepsilon, \nu)$  in der Tabelle auf Seite 58 definierten Relationen für die Operation von  $f$  auf  $Q$  sowie den im Rahmen der Fallunterscheidung herausgearbeiteten generischen Relationen lassen sich jetzt für alle acht Einzelfälle jeweils  $2^{3+4 \cdot 4}$  durch die Exponentenvektoren  $\alpha$ ,  $\beta$ ,  $\gamma$  und  $\delta$  parametrisierte endliche Präsentationen bauen. Mit Hilfe der MAGMA-Implementierung des Todd-Coxeter-Algorithmus wurde in circa  $4 \cdot 336$  CPU-Stunden<sup>1</sup> ermittelt, dass *nur acht(!)* der insgesamt  $2^{22} = 4194304$  korrespondierenden Gruppen die für eine Erweiterung  $J : S_5$  zu erwartende Ordnung  $2^{14} \cdot 3 \cdot 5 = 245760$  aufweisen, nämlich je vier zu den in der Tabelle auf Seite 58 fett gedruckten Exponentenvektorraaren  $(\varepsilon, \nu)$ .

Die Präsentationen dieser acht Zentralisatoren in spe unterscheiden sich voneinander lediglich anhand folgender Relationenmengen:

$$\mathcal{H}_1 := \{x_1^f = x_1w, \quad x_2^f = x_2ztw_1\} \quad \text{bzw.} \quad \mathcal{H}_2 := \{x_1^f = x_1tvw_1, \quad x_2^f = x_2ztv\}$$

und

$$\mathcal{H}_{11} := \{a^f = x_2bcdt, \quad b^f = dw_1, \quad c^f = x_1abtw_1, \quad d^f = cd\},$$

$$\mathcal{H}_{12} := \{a^f = x_2bcdzt, \quad b^f = dzw_1, \quad c^f = x_1abtw_1, \quad d^f = cd\},$$

---

<sup>1</sup>Vier PCs des Instituts für Experimentelle Mathematik mit 450 MHz Pentium-III-Prozessor und 512 MB Arbeitsspeicher waren über circa zwei Wochen hinweg parallel im Einsatz.

$$\begin{aligned}
\mathcal{H}_{13} &:= \{ a^f = x_2bcdv, \quad b^f = dvw_1, \quad c^f = x_1abtvw, \quad d^f = cdtvw_1 \}, \\
\mathcal{H}_{14} &:= \{ a^f = x_2bcdzv, \quad b^f = dzvw_1, \quad c^f = x_1abtvw, \quad d^f = cdtvw_1 \}, \\
\mathcal{H}_{21} &:= \{ a^f = x_2bcdw, \quad b^f = dzvw_1, \quad c^f = x_1abtvw_1, \quad d^f = cdztvw \}, \\
\mathcal{H}_{22} &:= \{ a^f = x_2bcdzw, \quad b^f = dvw_1, \quad c^f = x_1abtvw_1, \quad d^f = cdztvw \}, \\
\mathcal{H}_{23} &:= \{ a^f = x_2bcdtvw, \quad b^f = dzw_1, \quad c^f = x_1abztw, \quad d^f = cdww_1 \}, \\
\text{bzw. } \mathcal{H}_{24} &:= \{ a^f = x_2bcdztvw, \quad b^f = dw_1, \quad c^f = x_1abztw, \quad d^f = cdww_1 \}.
\end{aligned}$$

Unter Verwendung der in Satz 5.1.3 eingeführten Bezeichnungen definieren wir damit schließlich für jedes Indexpaar  $(i, j) \in \{1, 2\} \times \{1, 2, 3, 4\}$  die Gruppe

$$H_{ij} := \langle \mathcal{X}, f \mid \mathcal{S}, f^5 = 1, y^f = yy_2fy_2f, y_2^f = yfy_2, u^f = yufy_2f^2, \mathcal{H}_i, \mathcal{H}_{ij} \rangle.$$

Die Erzeugersubstitution  $d \mapsto dz$  transformiert  $\mathcal{H}_{i1}$  in  $\mathcal{H}_{i2}$  und  $\mathcal{H}_{i3}$  in  $\mathcal{H}_{i4}$  ( $i=1,2$ ), hat aber offensichtlich keinerlei Einfluss auf die Relationenmengen  $\mathcal{H}_1, \mathcal{H}_2$  oder  $\mathcal{S}$ , wo  $d$  allenfalls als Kommutatorkomponente vorkommt. Somit ist klar, dass

$$H_{11} \cong H_{12}, \quad H_{13} \cong H_{14}, \quad H_{21} \cong H_{22} \quad \text{und} \quad H_{23} \cong H_{24}. \quad (\text{E})$$

In der Tat lässt sich sogar noch mehr zeigen.

### Satz 5.1.9

Alle acht Gruppen  $H_{ij}$ ,  $i = 1, 2$ ,  $j = 1, 2, 3, 4$ , sind paarweise isomorph zueinander.

**Beweis.** Wegen (E) reicht es aus, die jeweilige Isomorphie von  $H_{13}$ ,  $H_{21}$  und  $H_{23}$  zur Gruppe  $H_{11}$  nachzuweisen. Das Abzählen der Nebenklassen von  $\langle y, y_2, u, f \rangle$  in  $H_{11}$  mit Hilfe des in MAGMA implementierten Todd-Coxeter-Algorithmus liefert eine treue Permutationsdarstellung  $\pi_{11} : H_{11} \hookrightarrow S_{2048}$ ; völlig analog erhält man entsprechende Einbettungen  $\pi_{13}$ ,  $\pi_{21}$  und  $\pi_{23}$ . Für  $\pi_{11}(H_{11})$  berechnet MAGMA ferner folgende endliche Präsentation:

$$\begin{aligned}
\pi_{11}(H_{11}) = \langle \mathfrak{d}, \eta_2, u, f \mid & \mathfrak{d}^2 = \eta_2^2 = u^2 = f^5 = 1, (\mathfrak{d}\eta_2)^4 = 1, \\
& \mathfrak{d}f u \mathfrak{d} u f^4 = 1, u f^3 \eta_2 f u f^4 = 1, \mathfrak{d} f \mathfrak{d}[u, \mathfrak{d}] f^4 = 1, \\
& f^4 \eta_2 f^4 u \eta_2 f u \eta_2 = 1, f u f \mathfrak{d} f^3 \mathfrak{d} \eta_2 \mathfrak{d} f^2 \mathfrak{d} u = 1, \\
& \eta_2 f[\eta_2, \mathfrak{d}] f^4 \mathfrak{d} f \eta_2 \mathfrak{d} \eta_2 f^4 \eta_2 \mathfrak{d} = 1, \\
& \mathfrak{d} \eta_2 u \mathfrak{d} \eta_2 \mathfrak{d} f \eta_2 \mathfrak{d} u \mathfrak{d} f^4 u \mathfrak{d} f^4 u = 1 \rangle.
\end{aligned}$$

Man verifiziert leicht, dass etwa

$$\mathfrak{d} = \pi_{11}(d), \quad \eta_2 = \pi_{11}(y_2), \quad u = \pi_{11}(u) \quad \text{und} \quad f = \pi_{11}(f)$$

in  $\pi_{11}(H_{11})$  paarweise nicht-konjugierte Elemente sind, welche die angegebenen Relationen erfüllen.

Tatsächlich findet MAGMA in jeder der Gruppen  $\pi_{13}(H_{13})$ ,  $\pi_{21}(H_{21})$  bzw.  $\pi_{23}(H_{23})$  ein Involutionentripel  $(\mathfrak{d}, \eta_2, u)$ , das vereint mit  $f = \pi_{13}(f)$ ,  $\pi_{21}(f)$  bzw.  $\pi_{23}(f)$  jenen Relationen genügt:

$$\left. \begin{aligned}
\mathfrak{d} &= \pi_{13}(yf^4y_2uyf^4y_2yy_2f^2bfu), \\
\eta_2 &= \pi_{13}(yf y_2 z v w), \\
u &= \pi_{13}(yf^4y_2uyfywf)
\end{aligned} \right\} \in \pi_{13}(H_{13}),$$

$$\begin{aligned}
& \left. \begin{aligned} \mathfrak{d} &= \pi_{21}(yzw_1bdy), \\ \eta_2 &= \pi_{21}(uyf^4y_2uyf^4y_2yf^2tft), \\ \mathfrak{u} &= \pi_{21}(uyf^4y_2uyfx_1fu) \end{aligned} \right\} \in \pi_{21}(H_{21}), \\
& \text{bzw.} \quad \left. \begin{aligned} \mathfrak{d} &= \pi_{23}(ubdu), \\ \eta_2 &= \pi_{23}(ufufzww_1), \\ \mathfrak{u} &= \pi_{23}(uyy_2zwy_2x_1) \end{aligned} \right\} \in \pi_{23}(H_{23}).
\end{aligned}$$

Daher ist die obige Präsentation für  $\pi_{11}(H_{11}) \cong H_{11}$  auch eine Präsentation für die Gruppen  $H_{13}$ ,  $H_{21}$  und  $H_{23}$ . Weil alle vier Gruppen dieselbe Ordnung besitzen, folgt die Behauptung.  $\square$

**Bemerkung:** Unter der zunächst freilich nur als Arbeitshypothese zulässigen Annahme, dass für die Rollen von  $\mathfrak{d}$ ,  $\eta_2$  bzw.  $\mathfrak{u}$  geeignete Involutionen im Falle ihrer Existenz in  $\pi_{13}(H_{13})$ ,  $\pi_{21}(H_{21})$  und  $\pi_{23}(H_{23})$  genau wie in  $\pi_{11}(H_{11})$  in paarweise verschiedenen Konjugiertenklassen der Längen 240, 480 und 640 liegen, fördert elementweises Durchsuchen dieser in jedem  $H_{ij}$  eindeutig bestimmten Klassen die gewünschten Tripel in relativ akzeptabler Rechenzeit zu Tage. Die „worst-case“-Abschätzung von  $240 \cdot 480 \cdot 640 = 73728000$  zu testenden Involutionentripeln pro Gruppe stellt sich im Vergleich zum praktischen Experiment als bei weitem zu pessimistisch heraus.

Mit der Permutationsgruppe  $H := \pi_{11}(H_{11})$  haben wir einen Eingabeparameter für den Michler-Algorithmus gefunden, der die Bedingungen (i)–(iii) aus Parrots Charakterisierung der Rudvalis-Gruppe erfüllt. Da allerdings eine Erzeugermenge mit 15 Elementen in gewissen Situationen relativ sperrig zu handhaben ist, identifizieren wir  $H$  nicht bloß mit  $H_{11}$ , sondern notieren zum Schluss dieses Abschnitts noch eine minimale Alternative.

### Satz 5.1.10

Unter Verwendung der bisher eingeführten Bezeichnungen gilt mit  $k := du$ :

$$H = \langle k, f \rangle.$$

**Beweis.** Trivialerweise ist  $\langle k, f \rangle \leq H$ . MAGMA's `InverseWordMap` liefert die entscheidende Faktorisierung für die umgekehrte Inklusion, nämlich

$$d = [k^2, f^4]k[f^4, k^2][fk^2f^4, k^{-1}]f[k^2, f]k^2[f, k]fk^2f^4k^{-1}f^4.$$

Aus der Präsentation von  $H_{11}$  liest man damit rekursiv ab:

$$\begin{aligned}
u &= dk, & y_2 &= f^2[u, f^4], & y &= [y_2, u], & c &= [d, u], & b &= [d, y_2], \\
a &= [c, y], & w_1 &= [b, c], & w &= [a, d], & t &= [a, y_2], & v &= [a, b]t, \\
z &= [d, t], & x_2 &= ba[d, y]tv, & x_1 &= [u, x_2].
\end{aligned}$$

$\square$

## 5.2 Start des Michler-Algorithmus

Das Pre-processing des Eingabeparameters (vergleiche Unterabschnitt 2.2.1) erledigt sich fast von selbst. Ein MAGMA-Einzeiler bestätigt, dass  $\mathbf{Z}(H) = \langle z \rangle$ , also zyklisch der Ordnung 2 ist. Es liegt deshalb nahe, Parrots 2-Sylowuntergruppe  $S$  von  $H$  zu fixieren und bezüglich der 2-zentralen Involution bleibt uns ohnehin keine andere Wahl als  $z \in S$ .



Erwartungsgemäß wenig Mühe bereitet Schritt 1 des Michler-Algorithmus. Ein Blick zurück auf Lemma 5.1.4(b) lässt immerhin vermuten, wo die Lösung dieser Aufgabe zu suchen ist.

**Lemma 5.2.1**

Die Gruppe  $A = \langle z, t, v, w, a \rangle$  ist der einzige elementar abelsche Normalteiler in  $S$  von maximaler Ordnung  $|A| \geq 4$  in Bezug auf die folgenden zwei Eigenschaften:

- (a)  $D := \mathbf{N}_H(A) < H$ ; denn es gilt  $D = S$ .
- (b)  $C := \mathbf{C}_H(A)$  hat eine 2-Gruppe als Zentrum; denn es gilt  $C = A = \mathbf{Z}(C)$ .

**Beweis.** Mit MAGMA verifiziert man die Teilaussagen (a) und (b). Laut Lemma 5.1.4(b) sind  $A$  und  $B$  die elementar abelschen Normalteiler maximaler Ordnung in  $S$ . Per Konstruktion ist  $B$  jedoch sogar normal in  $H$ , woraus die Behauptung folgt.  $\square$

In der Nomenklatur des Michler-Algorithmus formuliert heißt das  $\mathfrak{A} = \{A\}$ , Schritt 2 muss demnach genau *einmal* ausgeführt werden.

Hierzu fassen wir  $A$  als  $\text{GF}(2)$ -Vektorraum der Dimension  $d = \log_2 |A| = 5$  auf. Bezüglich der geordneten Basis  $(z, t, v, w, a)$  von  $A$  induziert die Konjugationsoperation von  $D$  auf  $A$  einen Homomorphismus  $\eta : D \rightarrow \text{GL}_5(2)$  mit Kern  $C$  und

$$\begin{aligned} \eta(w_1) &= \begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ 0 & 0 & 1 & & \\ 0 & 0 & 0 & 1 & \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}, & \eta(x_1) &= \begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ 0 & 0 & 1 & & \\ 0 & 0 & 0 & 1 & \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}, & \eta(x_2) &= \begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ 0 & 0 & 1 & & \\ 0 & 0 & 0 & 1 & \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \\ \eta(b) &= \begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ 0 & 0 & 1 & & \\ 1 & 0 & 0 & 1 & \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}, & \eta(y) &= \begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ 0 & 0 & 1 & & \\ 0 & 1 & 0 & 1 & \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, & \eta(y_2) &= \begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ 0 & 0 & 1 & & \\ 0 & 1 & 1 & 1 & \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \\ \eta(c) &= \begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ 1 & 0 & 1 & & \\ 0 & 0 & 0 & 1 & \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, & \eta(u) &= \begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ 0 & 1 & 1 & & \\ 0 & 0 & 0 & 1 & \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, & \eta(d) &= \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 0 & 0 & 1 & & \\ 0 & 0 & 0 & 1 & \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}. \end{aligned}$$

Anhand dieses Tableaus überzeugt man sich auch ohne Computer unschwer davon, dass

**Lemma 5.2.2**

$$\Delta := \eta(D) = \left\{ \begin{pmatrix} 1 & & & & \\ \varepsilon & 1 & & & \\ * & * & 1 & & \\ * & * & * & 1 & \\ * & * & * & \varepsilon & 1 \end{pmatrix} \middle| \varepsilon \in \{0, 1\} \right\} \leq \text{GL}_5(2).$$

Nun steht die Bestimmung der Menge  $\mathfrak{S}(A)$  aller Matrixgruppen  $\Phi \leq \text{GL}_5(2)$  von maximaler Ordnung bezüglich der in Unterabschnitt 2.2.3 genannten Bedingungen (a)–(c) auf dem Programm. Ein paar Vorüberlegungen theoretischer Natur sind notwendig, um den anfallenden Rechenaufwand in Grenzen zu halten.

### 5.3 Normalisatorerweiterung gesucht

Wie dem Atlas [8] der einfachen endlichen Gruppen zu entnehmen ist, besitzt  $L := \text{GL}_5(2)$  exakt fünf maximale Untergruppen, von denen aber wegen  $|\Delta| = 2^9$  bis auf Konjugiertheit in  $\mathbf{N}_L(\Delta)$  lediglich vier das Bild  $\Delta = \eta(D)$  beherbergen können:

$$\begin{array}{cccc}
 \left( \begin{array}{c|ccc} 1 & 0 & 0 & 0 & 0 \\ * & \boxed{L_4(2)} & & & \\ * & & & & \\ * & & & & \\ * & & & & \end{array} \right) & \left( \begin{array}{c|ccc} \boxed{S_3} & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ * & * & & \\ * & * & \boxed{L_3(2)} & \\ * & * & & \end{array} \right) & \left( \begin{array}{c|cc} \boxed{L_3(2)} & 0 & 0 \\ & 0 & 0 \\ * & * & * \\ * & * & * \\ & \boxed{S_3} & \end{array} \right) & \left( \begin{array}{c|ccc} \boxed{L_4(2)} & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ * & * & * & * \\ & & & 1 \end{array} \right) \\
 2^4 : L_4(2) & 2^6 : (S_3 \times L_3(2)) & 2^6 : (L_3(2) \times S_3) & 2^4 : L_4(2)
 \end{array}$$

Von links nach rechts handelt es sich dabei gerade um die Normalisatoren  $\mathbf{N}_L(E_1)$ ,  $\mathbf{N}_L(R_1)$ ,  $\mathbf{N}_L(R_2)$  bzw.  $\mathbf{N}_L(E_2)$  der elementar abelschen Untergruppen

$$E_1 := \left\{ \left( \begin{array}{c|c} 1 & \mathbf{0} \\ * & I_4 \end{array} \right) \right\}, \quad R_1 := \left\{ \left( \begin{array}{c|c} I_2 & \mathbf{0} \\ * & I_3 \end{array} \right) \right\}, \quad R_2 := \left\{ \left( \begin{array}{c|c} I_3 & \mathbf{0} \\ * & I_2 \end{array} \right) \right\}, \quad E_2 := \left\{ \left( \begin{array}{c|c} I_4 & \mathbf{0} \\ * & 1 \end{array} \right) \right\}$$

des Universums  $L$ . Für  $i \in \{1, 2\}$  betrachten wir außerdem  $F_i := \Delta \cap E_i$ .

Aufgrund der speziellen Gestalt der Elemente von  $\Delta$  (siehe Lemma 5.2.2) wird sofort klar, dass  $R_i \triangleleft \mathbf{C}_L(F_i)$  mit Index  $|\mathbf{C}_L(F_i) : R_i| = 2$  sowie  $\mathbf{N}_L(F_i) \leq \mathbf{N}_L(R_i)$ ,  $i = 1, 2$ . Folglich sollte jede Obergruppe  $\Phi \in \mathfrak{S}(A)$  von  $\Delta$  in  $N_1 := \mathbf{N}_L(R_1)$  oder  $N_2 := \mathbf{N}_L(R_2)$  zu finden sein.

#### Lemma 5.3.1

Für alle  $\Phi \in \mathfrak{S}(A)$  gilt  $|\Phi : \Delta| = 3$ .

**Beweis.** Falls  $\mathfrak{S}(A) = \emptyset$ , ist die Behauptung trivial. Ohne Beschränkung der Allgemeinheit sei daher  $N_1 \geq \Phi \in \mathfrak{S}(A)$ ; im Fall  $N_2 \geq \Phi$  greifen symmetrische Argumente.

Gewiss gilt  $|\Phi : \Delta| \in \{3, 7, 9, 21, 63\}$ , denn  $N_1$  hat die Ordnung  $|N_1| = 2^{10} \cdot 3^2 \cdot 7$  und  $\Delta$  gemäß der Definition von  $\mathfrak{S}(A)$  ungeraden Index in  $\Phi$ .

Angenommen, es existiert eine Matrix  $s \in \Phi$  mit  $\text{ord}(s) = 7$ . Weil  $s$  die Gruppe  $R_1$  normalisiert, wäre dann ohne Einschränkung

$$s \in L_1 := \left( \begin{array}{c|c} \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} & \mathbf{0} \\ \hline \mathbf{0} & \boxed{L_3(2)} \end{array} \right) \cong L_3(2).$$

In Gruppen vom Typ  $L_3(2)$  erzeugt eine Kleinsche Vierergruppe zusammen mit einem Element der Ordnung 7 stets schon die gesamte Gruppe.

$$\Delta \cap L_1 = \left\{ \left( \begin{array}{c|c} \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} & \mathbf{0} \\ \hline \mathbf{0} & \begin{array}{ccc} 1 & 0 & 0 \\ * & 1 & 0 \\ * & 0 & 1 \end{array} \end{array} \right) \right\} \cong 2^2$$

erzwingt deshalb  $L_1 = \langle \Delta \cap L_1, s \rangle \leq \Phi$ . Mit  $L_1$  würden jedoch auch alle unteren Dreiecksmatrizen, insbesondere also eine komplette 2-Sylowuntergruppe von  $L$  in  $\Phi$  liegen — ein Widerspruch zu  $\text{ggT}(|\Phi : \Delta|, 2) = 1$ . Es folgt  $|\Phi : \Delta| \in \{3, 9\}$ .

Wäre  $|\Phi : \Delta| = 9$ , so enthielte  $\Phi$  eine komplette 3-Sylowuntergruppe von  $N_1$ , das heißt unter anderem Elemente der Form

$$\left( \begin{array}{c|c} I_2 & \mathbf{0} \\ \hline * & T \end{array} \right) \quad \text{mit } T \in \text{GL}_3(2), \text{ ord}(T) = 3,$$

welche den ersten Basisvektor  $z \in A$  stabilisieren — im Widerspruch zur Definition von  $\mathfrak{S}(A)$ . Die einzig verbleibende Möglichkeit ist  $|\Phi : \Delta| = 3$ .  $\square$

Eine neuerliche Analyse des Matrizen-Tableaus auf Seite 67 lässt erkennen, dass

$$R_2 = \eta(\langle w_1, x_1, x_2, b, y, y_2 \rangle) \triangleleft \Delta \leq N_2$$

und  $K_0 := \eta(\langle c, u, d \rangle)$  ein Komplement von  $R_2$  in  $\Delta$  ist. Vor diesem Hintergrund wirkt das folgende Resultat etwas weniger überraschend:

**Lemma 5.3.2**

*Bis auf Konjugation in  $\mathbf{N}_L(\Delta)$  enthält die Menge  $\mathfrak{S}(A)$  höchstens ein Element, nämlich*

$$\Phi_0 := \langle \Delta, \mathfrak{T}_0 \rangle \leq N_2 \quad \text{mit} \quad \mathfrak{T}_0 := \left( \begin{array}{ccc|cc} 1 & 1 & 0 & & \\ 1 & 0 & 0 & & \mathbf{0} \\ 0 & 0 & 1 & & \\ \hline & & & 1 & 1 \\ \mathbf{0} & & & 1 & 0 \end{array} \right).$$

**Beweis.** Für  $\mathfrak{S}(A) = \emptyset$  ist die Behauptung trivialerweise wahr. Sei daher  $\Phi \in \mathfrak{S}(A)$ .

Angenommen,  $\Phi \leq N_1$ . Wegen Lemma 5.3.1 gilt dann  $\Phi = \langle \Delta, \mathfrak{T} \rangle$  mit einer Matrix

$$\mathfrak{T} = \mathfrak{T}(T_0, T_1, T_2) = \left( \begin{array}{c|ccc} T_1 & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ \hline T_0 & & & T_2 \end{array} \right) \in L$$

der Ordnung 3. Darüber hinaus verlangt der Michler-Algorithmus  $\mathfrak{T} \notin \text{Stab}_\Phi(z)$ , so dass

$$T_1 \in \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \subset \text{GL}_2(2) \cong S_3$$

bereits gesichert ist, während  $T_2 \in \text{GL}_3(2)$  prinzipiell sowohl die Einheitsmatrix  $I_3$  als auch ein Block der Ordnung 3 sein könnte. Die Variante  $T_2 = I_3$  ist freilich ein Spezialfall der Situation  $\Phi \leq N_2$ , weshalb wir an dieser Stelle ohne Einschränkung von  $\text{ord}(T_2) = 3$  ausgehen dürfen.

Es bezeichne  $\tilde{\cdot} : N_1 \rightarrow \tilde{N}_1$  die Projektion der Elemente von  $N_1$  auf ihren rechten unteren  $3 \times 3$ -Block. Dann gilt  $\tilde{N}_1 \cong L_3(2)$  und  $\tilde{\Phi} < \tilde{N}_1$  mit  $|\tilde{\Phi}| = 2^3 \cdot 3$ . Der direkte Vergleich mit den maximalen Untergruppen von  $L_3(2)$  ergibt  $\tilde{\Phi} \cong S_4$ .

Aus Ordnungsgründen überträgt sich ebendiese Isomorphiebeziehung in die Faktorgruppe  $\bar{N}_1 := N_1/R_1$ ; vermöge der Querstrichkonvention gilt also  $\bar{\Phi} \cong S_4$  und infolgedessen wiederum

$$\langle \bar{\eta}(w_1 x_2) \rangle = \left\{ \left( \begin{array}{cc|ccc} 1 & 0 & & & & \\ 0 & 1 & & & & \mathbf{0} \\ \hline & & 1 & 0 & 0 \\ \mathbf{0} & & 0 & 1 & 0 \\ & & * & 0 & 1 \end{array} \right) \right\} = \mathbf{Z}(\bar{\Delta}) \leq O_2(\bar{\Phi}).$$

Da man, abhängig von  $T_1$ , entweder  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  oder  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  als linken oberen  $2 \times 2$ -Block von  $\eta(d)^{\mathfrak{T}}$  ermittelt, ist

$$\bar{\eta}(d)^{\bar{\mathfrak{T}}} \notin \langle \bar{\eta}(w_1x_2), \bar{\eta}(d) \rangle \quad \text{bzw.} \quad \langle \bar{\eta}(w_1x_2), \bar{\eta}(d) \rangle \neq O_2(\bar{\Phi}) .$$

Vielmehr gilt  $O_2(\bar{\Phi}) = \langle \bar{\eta}(w_1x_2), \bar{\eta}(x_1yy_2) \rangle$ , denn

$$\eta(x_1yy_2) = \bar{\eta}(x_1yy_2) = \left( \begin{array}{cc|ccc} 1 & 0 & & & \\ 0 & 1 & & & \\ \hline & & 1 & 0 & 0 \\ & & 1 & 1 & 0 \\ & & 0 & 0 & 1 \end{array} \right) ,$$

Es folgt  $O_2(\Phi) = R_1R_2$ . Weil  $R_1$  und  $R_2$  mithin die einzigen elementar abelschen Untergruppen der Ordnung  $2^6$  in  $O_2(\Phi)$  sind, muss  $\mathfrak{T}$  tatsächlich alle *beide* normalisieren, das bedeutet  $\mathfrak{T} \in \Phi \leq N_2$ .

Fortan bezeichne  $\hat{\cdot}: N_2 \rightarrow \hat{N}_2$  bzw.  $\check{\cdot}: N_2 \rightarrow \check{N}_2$  die Projektion der Elemente von  $N_2$  auf ihren linken oberen  $3 \times 3$ - bzw. ihren rechten unteren  $2 \times 2$ -Block. Ferner bezieht sich die Querstrichkonvention ab jetzt auf die Faktorgruppe  $\bar{N}_2 := N_2/R_2$ .

Wegen Lemma 5.3.1 ist

$$\bar{\Delta} = \langle \bar{\eta}(c), \bar{\eta}(u), \bar{\eta}(d) \rangle \cong D_8$$

eine Untergruppe vom Index 3 in  $\bar{\Phi} \leq \bar{N}_2$ . Wie schon zuvor liefert ein Vergleich von  $|\hat{\Phi}| = 2^3 \cdot 3$  mit den Ordnungen der maximalen Untergruppen von  $L_3(2) \cong \hat{N}_2$  die Beziehung  $\hat{\Phi} \cong S_4$ . Andererseits haben wir  $\check{\eta}(d) \neq I_2$ , so dass  $\bar{\Phi}$  insgesamt isomorph zu einer Untergruppe im direkten Produkt  $S_4 \times S_3$  ist.

Gewiss findet man aber keine Untergruppe vom Typ  $2^2 \times 3$  in  $\bar{\Phi}$ , da ein zugehöriges Element der Ordnung 3 im Kern der Projektion  $\hat{\cdot}$  läge und somit den ersten Basisvektor  $z \in A$  stabilisieren würde — ein Widerspruch zur Definition von  $\mathfrak{S}(A)$ .

Insbesondere gilt

$$\Phi \cap R_2 \left( \begin{array}{ccc|ccc} 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ \hline & & & \mathbf{0} & & \\ & & & & \boxed{S_3} & \end{array} \right) = R_2 ,$$

woraus  $\bar{\Phi} \cong S_4$  folgt und deshalb wiederum

$$\langle \bar{\eta}(c) \rangle = \mathbf{Z}(\bar{\Delta}) \leq O_2(\bar{\Phi}) .$$

Angenommen,  $O_2(\bar{\Phi}) = \langle \bar{\eta}(c), \bar{\eta}(d) \rangle$ . Im Widerspruch zur Definition von  $\mathfrak{S}(A)$  müsste  $\mathfrak{T}$  dann den ersten Basisvektor  $z \in A$  stabilisieren, denn es wäre

$$\mathbf{N}_{\text{GL}_3(2)}(O_2(\hat{\Phi})) = \left( \begin{array}{ccc|ccc} 1 & 0 & 0 & & & \\ * & & & & & \\ * & & & & \boxed{S_3} & \end{array} \right) .$$

Dies impliziert  $O_2(\bar{\Phi}) = \langle \bar{\eta}(c), \bar{\eta}(u) \rangle$ . Aufgrund der zur Gegendiagonalen symmetrischen Struktur von  $\eta(d)$  verbleiben damit für  $\mathfrak{T}$  ohne Einschränkung noch genau

drei Möglichkeiten:

$$\mathfrak{T} = \mathfrak{T}_0, \quad \mathfrak{T} = \mathfrak{T}_1 := \left( \begin{array}{ccc|c} 0 & 1 & 0 & \\ 1 & 1 & 0 & \mathbf{0} \\ 0 & 0 & 1 & \\ \hline & & & 1 & 1 \\ & & & 1 & 0 \end{array} \right) \quad \text{oder} \quad \mathfrak{T} = \mathfrak{T}_2 := \left( \begin{array}{ccc|c} 1 & 1 & 0 & \\ 1 & 0 & 0 & \mathbf{0} \\ 0 & 0 & 1 & \\ \hline & & & 1 & 0 \\ & & & 0 & 1 \end{array} \right).$$

Für  $\mathfrak{T} = \mathfrak{T}_1, \mathfrak{T}_2$  erhält man jedoch mit  $\eta(w_1)^{\mathfrak{T}_1} = \eta(x_1y)$  und  $\eta(w_1)^{\mathfrak{T}_2} = \eta(w_1x_1)$  Konjugationsübergänge ohne Urbild in  $D$ . Während sich nämlich die Linksnebenklasse  $w_1A$  zur Hälfte aus Involutionen zusammensetzt, sind sowohl in  $x_1yA$  als auch in  $w_1x_1A$  ausschließlich Elemente der Ordnung 4 anzutreffen.  $\square$

Ob die Gruppe  $\Phi_0 = \langle \Delta, \mathfrak{T}_0 \rangle$  wirklich in  $\mathfrak{S}(A)$  liegt, hängt allein davon ab, ob es gelingt, die Präsentation von  $D = S$  zur Präsentation mindestens einer Erweiterungsgruppe  $E_\Phi = \langle D, t_0 \rangle$  auszubauen.

Wie der Extra-Erzeuger  $t_0$  mit  $t_0^3 = 1$  auf dem elementar abelschen Normalteiler  $A$  von  $S$  agiert, können wir unmittelbar an der Matrix  $\mathfrak{T}_0$  ablesen. Demnach gelten die Relationen in

$$\mathcal{T}_A := \{ z^{t_0} = zt, \quad t^{t_0} = z, \quad v^{t_0} = v, \quad w^{t_0} = wa, \quad a^{t_0} = w \}.$$

Hingegen wird die Konjugationswirkung von  $t_0$  auf den übrigen Erzeugern von  $S$  durch ihr Abbild unter  $\eta$ , das heißt durch die Operation von  $\mathfrak{T}_0$  auf  $\Delta$ , nur modulo  $C = A$  beschrieben:

$$\begin{aligned} \eta(w_1)^{\mathfrak{T}_0} &= \eta(x_2by), & \eta(b)^{\mathfrak{T}_0} &= \eta(yy_2x_1b), & \eta(y)^{\mathfrak{T}_0} &= \eta(w_1), \\ \eta(y_2)^{\mathfrak{T}_0} &= \eta(x_1b), & \eta(x_1b)^{\mathfrak{T}_0} &= \eta(by_2x_2by), & \eta(x_2by)^{\mathfrak{T}_0} &= \eta(y), \\ \eta(c)^{\mathfrak{T}_0} &= \eta(cu), & \eta(u)^{\mathfrak{T}_0} &= \eta(c), & \mathfrak{T}_0^{\eta(d)} &= \mathfrak{T}_0^2. \end{aligned}$$

Um diese Gleichungen in einen Satz exakter und konsistenter Relationen für eine potentielle Erweiterungsgruppe  $E_\Phi$  zu transformieren, empfiehlt sich folgendes systematische Vorgehen:

1. Streiche alle Abbildungsklammern „ $\eta(\dots)$ “ und ersetze  $\mathfrak{T}_0$  überall durch  $t_0$ .
2. Ergänze auf der rechten Seite jeder Relation  $g^{t_0} = r$  ein geeignetes Element  $e_g \in A$ .

Indem wir auch für die Linksnebenklassen  $x_2byA$  und  $x_1bA$  Repräsentanten der Ordnung 2 benutzen, etwa  $x_2bya$  und  $x_1baw$ , sind wir mit Hilfe von MAGMA in der Lage, die Menge der als „geeignet“ in Frage kommenden Elemente  $e_g$  analog zu Lemma 5.1.8 auszudünnen.

- $\text{ord}(x_2bya) = 2$ ; also gilt

$$w_1^{t_0} = x_2bya \cdot e_{w_1} \tag{F}$$

für ein  $e_{w_1} \in \mathbf{C}_A(x_2bya) = \mathbf{C}_A(x_2by) = \langle z, t, v, wa \rangle$ .

Mit Exponentenvektor  $\nu \in \{0, 1\}^4$  ist der Faktor  $e_{w_1}$  deshalb von der Gestalt

$$e_{w_1} = z^{\nu_1} t^{\nu_2} v^{\nu_3} (wa)^{\nu_4}.$$

- $\text{ord}(yy_2x_1baw) = 2$ ; also gilt

$$b^{t_0} = yy_2x_1baw \cdot e_b \tag{G}$$

für ein  $e_b \in \mathbf{C}_A(yy_2x_1baw) = \mathbf{C}_A(yy_2x_1b) = \langle z, t, v \rangle$ .

Mit Exponentenvektor  $\nu \in \{0, 1\}^3$  ist der Faktor  $e_b$  deshalb von der Gestalt

$$e_b = z^{\nu_1} t^{\nu_2} v^{\nu_3}.$$

- $\text{ord}(w_1) = 2$ ; also gilt

$$y^{t_0} = w_1 \cdot e_y \quad (\text{H})$$

für ein  $e_y \in \mathbf{C}_A(w_1) = \langle z, t, v, w \rangle$ .

Mit Exponentenvektor  $\nu \in \{0, 1\}^4$  ist der Faktor  $e_y$  deshalb von der Gestalt

$$e_y = z^{\nu_1} t^{\nu_2} v^{\nu_3} w^{\nu_4} .$$

- $\text{ord}(x_1 baw) = 2$ ; also gilt

$$y_2^{t_0} = x_1 baw \cdot e_{y_2} \quad (\text{I})$$

für ein  $e_{y_2} \in \mathbf{C}_A(x_1 baw) = \mathbf{C}_A(x_1 b) = \langle z, t, v \rangle$ .

Mit Exponentenvektor  $\nu \in \{0, 1\}^3$  ist der Faktor  $e_{y_2}$  deshalb von der Gestalt

$$e_{y_2} = z^{\nu_1} t^{\nu_2} v^{\nu_3} .$$

- $\text{ord}(by_2 x_2 bya) = 2$ ; also gilt

$$(x_1 baw)^{t_0} = by_2 x_2 bya \cdot e_{x_1 baw} \quad (\text{J})$$

für ein  $e_{x_1 baw} \in \mathbf{C}_A(by_2 x_2 bya) = \mathbf{C}_A(by_2 x_2 by) = \langle z, t, v \rangle$ .

Mit Exponentenvektor  $\nu \in \{0, 1\}^3$  ist der Faktor  $e_{x_1 baw}$  deshalb von der Gestalt

$$e_{x_1 baw} = z^{\nu_1} t^{\nu_2} v^{\nu_3} .$$

- $\text{ord}(y) = 2$ ; also gilt

$$(x_2 bya)^{t_0} = y \cdot e_{x_2 bya} \quad (\text{K})$$

für ein  $e_{x_2 bya} \in \mathbf{C}_A(y) = \langle z, t, v, a \rangle$ .

Mit Exponentenvektor  $\nu \in \{0, 1\}^4$  ist der Faktor  $e_{x_2 bya}$  deshalb von der Gestalt

$$e_{x_2 bya} = z^{\nu_1} t^{\nu_2} v^{\nu_3} a^{\nu_4} .$$

- $\text{ord}(cu) = 2$ ; also gilt

$$c^{t_0} = cu \cdot e_c \quad (\text{L})$$

für ein  $e_c \in \mathbf{C}_A(cu) = \langle z, t, w, a \rangle$ .

Mit Exponentenvektor  $\nu \in \{0, 1\}^4$  ist der Faktor  $e_c$  deshalb von der Gestalt

$$e_c = z^{\nu_1} t^{\nu_2} w^{\nu_3} a^{\nu_4} .$$

- $\text{ord}(c) = 2$ ; also gilt

$$u^{t_0} = c \cdot e_u \quad (\text{M})$$

für ein  $e_u \in \mathbf{C}_A(c) = \langle z, t, w, a \rangle$ .

Mit Exponentenvektor  $\nu \in \{0, 1\}^4$  ist der Faktor  $e_u$  deshalb von der Gestalt

$$e_u = z^{\nu_1} t^{\nu_2} w^{\nu_3} a^{\nu_4} .$$

Vergessen werden darf außerdem nicht, dass

$$t_0^d = t_0^2 \cdot e_{t_0} \quad (\text{N})$$

für ein Wort  $e_{t_0} = e_{t_0}(z, t, v, w, a) \in A$  gilt. Von den ursprünglich  $2^{5 \cdot 9}$  überhaupt denkbaren Faktorkombinationen sind daher lediglich  $2^{4 \cdot 5 + 3 \cdot 3 + 5}$  zu testen. Zweifellos befindet sich aber selbst dieses Vorhaben noch jenseits des technisch in akzeptabler Zeit Machbaren.

Dank der Schichtenstruktur der Faktorgruppe  $D/C = S/A \cong 2^6 : D_8$  lässt sich das Problem allerdings hervorragend durch eine „divide et impera“-Strategie knacken!

#### □ Der schwere Part

Aus dem für  $\langle A, x_1, x_2, w_1, b, y, y_2 \rangle$  relevanten Teil der Präsentation von  $S$ , der Relationenmenge  $\mathcal{T}_A$  und den generischen Relationen (F)–(K) konstruieren wir zunächst  $2^{4 \cdot 3 + 3 \cdot 3}$  durch Exponentenvektoren parametrisierte endliche Präsentationen, die zerfallende Erweiterungen der Struktur  $(A.2^6) : 3$  bzw. epimorphe Bilder davon definieren.

Die MAGMA-Implementierung des Todd-Coxeter-Algorithmus berechnete in circa 4·144 CPU-Stunden, dass nur 4096 der insgesamt  $2^{21} = 2097152$  betrachteten Gruppen die zu erwartende Ordnung  $2^{11} \cdot 3 = 6144$  aufweisen. Die korrespondierenden Exponentenvektoren wurden zur späteren Weiterverwendung abgespeichert<sup>2</sup>.

#### □ Der leichte Part

Aus dem für  $\langle A, c, u, d \rangle$  relevanten Teil der Präsentation von  $S$ , der Relationenmenge  $\mathcal{T}_A$  und den generischen Relationen (L)–(N) bauen wir sodann in einer zweiten Phase  $2^{4 \cdot 2 + 5}$  durch Exponentenvektoren parametrisierte endliche Präsentationen, die zerfallende Erweiterungen der Struktur  $A : (D_8.3)$  bzw. epimorphe Bilder davon definieren.

Die Analyse dieser  $2^{13} = 8192$  Gruppen erledigte MAGMA in knapp 15 CPU-Minuten. Nur 16 Exponentenvektoren führten zur maximal möglichen Ordnung  $2^8 \cdot 3 = 768$  und wurden zur späteren Weiterverwendung abgespeichert.

#### □ Die Fusion

Schließlich müssen die Präsentation von  $S$ , die Relationenmenge  $\mathcal{T}_A$  und die gesicherten Exponentenvektorsets kombiniert werden, um parametrisierte endliche Präsentationen zu erhalten, die zerfallende Erweiterungen  $(A.2^6) : S_4$  bzw. epimorphe Bilder davon definieren.

Innerhalb von 7 CPU-Stunden fand MAGMA unter den  $2^{12+4}$  zur Auswahl stehenden Gruppen genau 32 Exemplare der zu erwartenden Ordnung  $2^{14} \cdot 3 = 49152$ . Dabei treten jedoch nicht mehr als *acht essentiell verschiedene* Präsentationen auf, aus denen jeweils drei weitere durch Anwendung der Erzeugersubstitutionen  $d \mapsto dz$  oder/und  $u \mapsto uz$  hervorgehen. Die acht in diesem Sinne signifikanten Relationenteilmengen sind

$$\begin{aligned} \mathcal{E}_1 &:= \left\{ \begin{array}{l} w_1^{t_0} = x_2byw, \quad b^{t_0} = yy_2x_1bawv, \quad y^{t_0} = w_1zw, \quad y_2^{t_0} = x_1bawtv, \\ (x_1baw)^{t_0} = by_2x_2byazv, \quad (x_2bya)^{t_0} = yt, \quad t_0^d = t_0^2 \end{array} \right\}, \\ \mathcal{E}_2 &:= \left\{ \begin{array}{l} w_1^{t_0} = x_2byw, \quad b^{t_0} = yy_2x_1bawtv, \quad y^{t_0} = w_1w, \quad y_2^{t_0} = x_1baw, \\ (x_1baw)^{t_0} = by_2x_2byaztv, \quad (x_2bya)^{t_0} = y, \quad t_0^d = t_0^2wa \end{array} \right\}, \\ \mathcal{E}_3 &:= \left\{ \begin{array}{l} w_1^{t_0} = x_2byw, \quad b^{t_0} = yy_2x_1bawzv, \quad y^{t_0} = w_1zw, \quad y_2^{t_0} = x_1bawzv, \\ (x_1baw)^{t_0} = by_2x_2byav, \quad (x_2bya)^{t_0} = yt, \quad t_0^d = t_0^2 \end{array} \right\}, \\ \mathcal{E}_4 &:= \left\{ \begin{array}{l} w_1^{t_0} = x_2byw, \quad b^{t_0} = yy_2x_1bawztv, \quad y^{t_0} = w_1w, \quad y_2^{t_0} = x_1bawzt, \\ (x_1baw)^{t_0} = by_2x_2byatv, \quad (x_2bya)^{t_0} = y, \quad t_0^d = t_0^2wa \end{array} \right\}, \end{aligned}$$

<sup>2</sup>ASCII-Format, Platzbedarf rund 153 kB

$$\begin{aligned}
\mathcal{E}_5 &:= \left\{ \begin{array}{l} w_1^{t_0} = x_2bywzt, \quad b^{t_0} = yy_2x_1baw, \quad y^{t_0} = w_1zw, \quad y_2^{t_0} = x_1bawv, \\ (x_1baw)^{t_0} = by_2x_2bya, \quad (x_2bya)^{t_0} = y, \quad t_0^d = t_0^2wa \end{array} \right\}, \\
\mathcal{E}_6 &:= \left\{ \begin{array}{l} w_1^{t_0} = x_2bywzt, \quad b^{t_0} = yy_2x_1bawt, \quad y^{t_0} = w_1w, \quad y_2^{t_0} = x_1bawt, \\ (x_1baw)^{t_0} = by_2x_2byat, \quad (x_2bya)^{t_0} = yt, \quad t_0^d = t_0^2 \end{array} \right\}, \\
\mathcal{E}_7 &:= \left\{ \begin{array}{l} w_1^{t_0} = x_2bywzt, \quad b^{t_0} = yy_2x_1bawz, \quad y^{t_0} = w_1zw, \quad y_2^{t_0} = x_1bawz, \\ (x_1baw)^{t_0} = by_2x_2byaz, \quad (x_2bya)^{t_0} = y, \quad t_0^d = t_0^2wa \end{array} \right\}, \\
\text{und } \mathcal{E}_8 &:= \left\{ \begin{array}{l} w_1^{t_0} = x_2bywzt, \quad b^{t_0} = yy_2x_1bawzt, \quad y^{t_0} = w_1w, \quad y_2^{t_0} = x_1bawz, \\ (x_1baw)^{t_0} = by_2x_2byazt, \quad (x_2bya)^{t_0} = yt, \quad t_0^d = t_0^2 \end{array} \right\}.
\end{aligned}$$

Mit Rückgriff auf zwei bereits in Satz 5.1.3 eingeführte Bezeichnungen können wir nun für jedes  $i \in \{1, 2, \dots, 8\}$  die Gruppe

$$E_{\Phi}^{(i)} := \langle \mathcal{X}, t_0 \mid \mathcal{S}, t_0^3 = 1, c^{t_0} = cu, u^{t_0} = c, \mathcal{T}_A, \mathcal{E}_i \rangle. \quad (\text{O})$$

definieren und sämtliche Ergebnisse von Schritt 2 des Michler-Algorithmus bilanzieren:

**Satz 5.3.3**

Fixiert man das Tupel  $(z, t, v, w, a)$  als geordnete Basis des  $\text{GF}(2)$ -Vektorraums  $A$ , so gelten:

- (a) Die Konjugationsoperation von  $D = S$  auf  $A$  induziert einen Homomorphismus

$$\eta : D \rightarrow \Delta = \eta(D) \leq \text{GL}_5(2)$$

mit Kern  $C = A$  und Bild  $\Delta$  gemäß Lemma 5.2.2.

- (b) Die endliche Präsentation von  $D$  kann zu endlichen Präsentationen semidirekter Produkte von  $C$  mit der in Lemma 5.3.2 definierten Gruppe  $\Phi_0$  erweitert werden.
- (c) Die Gruppe  $\Phi_0$  ist das einzige Element der Zielmenge  $\mathfrak{S}(A)$ .
- (d) Bis auf Isomorphie gibt es genau eine Gruppenerweiterung

$$1 \rightarrow C \rightarrow E_{\Phi_0} \rightarrow \Phi_0 \rightarrow 1,$$

zu der eine Einbettung  $\mu : D \hookrightarrow E_{\Phi_0}$  existiert, so dass das Diagramm

$$\begin{array}{ccccccc}
1 & \longrightarrow & C & \longrightarrow & E_{\Phi_0} & \longrightarrow & \Phi_0 \longrightarrow 1 \\
& & \uparrow \text{Id}_C & & \uparrow \mu & & \uparrow \text{Id}_{\Phi} \\
1 & \longrightarrow & C & \xrightarrow{\text{Id}_D} & D & \xrightarrow{\eta} & \Delta \longrightarrow 1
\end{array}$$

kommutiert, nämlich  $E_{\Phi_0} \cong E_{\Phi}^{(1)}$ .

**Beweis.** Teilaussage (a) ist eine Inhaltsangabe von Abschnitt 5.2 und Behauptung (b) das Fazit der MAGMA-Berechnungen, welche die Definition (O) motiviert haben; schließlich folgt (c) aus (b) und Lemma 5.3.2, denn das maßgebliche Diagramm in (d) kommutiert mittels der kanonischen Injektion  $\mu : D \rightarrow D \leq E_{\Phi}^{(1)}$ .



Zu zeigen bleibt somit nurmehr Teil **(d)**:

Das Abzählen der Nebenklassen von  $\langle v, w, a, t_0 \rangle$  in  $E_{\Phi}^{(i)}$  mit Hilfe des in MAGMA implementierten Todd-Coxeter-Algorithmus liefert eine treue Permutationsdarstellung  $\pi_i : E_{\Phi}^{(i)} \hookrightarrow S_{2048}$ ,  $i = 1, 2, \dots, 8$ . Für  $\pi_1(E_{\Phi}^{(1)})$  bestimmt MAGMA ferner folgende endliche Präsentation:

$$\begin{aligned} \pi_1(E_{\Phi}^{(1)}) = \langle \mathfrak{d}, \eta_2, u, t_0 \mid & \mathfrak{d}^2 = \eta_2^2 = u^2 = t_0^3 = 1, (\mathfrak{d}\eta_2)^4 = 1, (\eta_2 u)^4 = 1, \\ & (\mathfrak{d}t_0^2)^2 = 1, (\mathfrak{d}t_0 u)^2 = 1, (t_0^2 u)^3 = 1, [\eta_2, t_0 u]^2 = 1, \\ & (\mathfrak{d}t_0 \eta_2 u \eta_2)^2 = 1, (\mathfrak{d}t_0 \eta_2)^3 t_0^2 \mathfrak{d} \eta_2 = 1, \\ & u t_0 [\eta_2, t_0^2] \eta_2 \mathfrak{d} t_0^2 \eta_2 u t_0^2 \eta_2 \mathfrak{d} = 1, \\ & \eta_2 t_0 u t_0 \eta_2 [t_0, \eta_2] u \eta_2 t_0 u = 1, \\ & u t_0^2 \eta_2 \mathfrak{d} t_0^2 \eta_2 t_0 \mathfrak{d} \eta_2 \mathfrak{d} u \eta_2 \mathfrak{d} \eta_2 t_0 = 1 \rangle. \end{aligned}$$

Man verifiziert leicht, dass etwa

$$\mathfrak{d} = \pi_1(d), \quad \eta_2 = \pi_1(y_2), \quad u = \pi_1(u) \quad \text{und} \quad t_0 = \pi_1(t_0)$$

in  $\pi_1(E_{\Phi}^{(1)})$  paarweise nicht-konjugierte Elemente sind, welche die angegebenen Relationen erfüllen.

Tatsächlich macht MAGMA in jeder der anderen Gruppen  $\pi_i(E_{\Phi}^{(i)})$ ,  $i = 2, 3, \dots, 8$ , ebenfalls ein Involutionentripel  $(\mathfrak{d}, \eta_2, u)$  ausfindig, das vereint mit  $t_0 = \pi_i(t_0)$  jenen Relationen genügt:

$$\begin{aligned} \left. \begin{array}{l} \mathfrak{d} = \pi_2(wavt_0^2 d), \\ \eta_2 = \pi_2(avy_2 x_2 y), \\ u = \pi_2(tcu) \end{array} \right\} & \in \pi_2(E_{\Phi}^{(2)}), \quad \left. \begin{array}{l} \mathfrak{d} = \pi_3(t_0^2 d), \\ \eta_2 = \pi_3(ax_2 y y_2), \\ u = \pi_3(wat_0^2 zct_0) \end{array} \right\} & \in \pi_3(E_{\Phi}^{(3)}), \\ \\ \left. \begin{array}{l} \mathfrak{d} = \pi_4(at_0^2 w_1 bdx_2), \\ \eta_2 = \pi_4(ayx_2 y_2), \\ u = \pi_4(wcu) \end{array} \right\} & \in \pi_4(E_{\Phi}^{(4)}), \quad \left. \begin{array}{l} \mathfrak{d} = \pi_5(aww_1 bx_2 d), \\ \eta_2 = \pi_5(vzy_2), \\ u = \pi_5(wau) \end{array} \right\} & \in \pi_5(E_{\Phi}^{(5)}), \\ \\ \left. \begin{array}{l} \mathfrak{d} = \pi_6(d), \\ \eta_2 = \pi_6(vy_2), \\ u = \pi_6(u) \end{array} \right\} & \in \pi_6(E_{\Phi}^{(6)}), \quad \left. \begin{array}{l} \mathfrak{d} = \pi_7(wvd), \\ \eta_2 = \pi_7(ty_2), \\ u = \pi_7(azu) \end{array} \right\} & \in \pi_7(E_{\Phi}^{(7)}), \\ \\ & \left. \begin{array}{l} \mathfrak{d} = \pi_8(vd), \\ \eta_2 = \pi_8(zty_2), \\ u = \pi_8(aztu) \end{array} \right\} & \in \pi_8(E_{\Phi}^{(8)}). \end{aligned}$$

Daher ist die obige Präsentation für  $\pi_1(E_{\Phi}^{(1)}) \cong E_{\Phi}^{(1)}$  auch eine Präsentation für die Gruppen  $E_{\Phi}^{(i)}$ ,  $i = 2, 3, \dots, 8$ . Weil alle acht Gruppen dieselbe Ordnung besitzen, folgt die Behauptung.  $\square$

**Bemerkung:** Unter der zunächst freilich nur als Arbeitshypothese zulässigen Annahme, dass für die Rollen von  $\mathfrak{d}$ ,  $\eta_2$  bzw.  $u$  geeignete Involutionen im Falle ihrer Existenz in  $\pi_i(E_{\Phi}^{(i)})$ ,  $i = 2, 3, \dots, 8$ , genau wie in  $\pi_1(E_{\Phi}^{(1)})$  in den paarweise verschiedenen Konjugiertenklassen von  $\pi_i(d)$ ,  $\pi_i(y_2)$  bzw.  $\pi_i(u)$  liegen, fördert elementweises Durchsuchen dieser Klassen die gewünschten Tripel in relativ akzeptabler Rechenzeit zu Tage.

Ohne Einschränkung identifizieren wir fortan  $E_\Phi := E_\Phi^{(1)}$  mit  $\pi_1(E_\Phi^{(1)})$ . Neben der im Beweis von Satz 5.3.3 erwähnten kanonischen Injektion  $\mu$  könnte es noch weitere Einbettungen von  $D$  in  $E_\Phi$  geben, welche das betreffende Gruppendiagramm kommutieren lassen. Da hier lediglich die *Existenz* der Rudvalis-Gruppe zur Debatte steht und die gewählte Einbettung  $\mu$  uns zum Ziel führt, werden wir auf derartige *Eindeutigkeitsfragen* nicht näher eingehen.

## 5.4 Kompatible Paare, Probleme und ein Ausweg

In Schritt 3 des Michler-Algorithmus sind allem anderen voran konkrete Charaktertafeln für die Gruppen  $H$ ,  $E_\Phi$ ,  $D = S$  und  $\mu(D) \leq E_\Phi$  zu berechnen. Als Permutationsgruppenargumente von moderater Ordnung und Grad dürfen wir sie mit gutem Gewissen der MAGMA-Implementierung des Dixon-Schneider-Algorithmus überlassen.

### 5.4.1 Experiment A: Klassische Darstellungstheorie

Um die Algorithmen 4.2.1 und 4.2.3 zur Ermittlung kompatibler Charakterpaare einsetzen zu können, standardisieren wir die Reihenfolge der Konjugiertenklassen von  $D$  und  $\mu(D)$  vermöge eines *simultanen* Repräsentantensystems. Spätestens an diesem Punkt wird absolut offenkundig, welche enormen Vorteile der konzeptionelle Ansatz,  $E_\Phi$  durch Erweiterung einer Präsentation von  $D$  zu konstruieren, mit sich bringt.

#### Satz 5.4.1

Die folgende Tabelle beschreibt ein Repräsentantensystem für die 85 Konjugiertenklassen der Gruppe  $D$ , bestehend aus den Vertreterworten  $\mathfrak{w}$  mit lexikographisch kleinster Basis bezüglich der Erzeugermenge  $\mathcal{X} = \{z, t, v, w, w_1, x_1, x_2, a, b, c, d, y, y_2, u\}$ :

Klasse	$\mathfrak{w}$	$ (\mathfrak{w})^D $	$ C_D(\mathfrak{w}) $	2P
1	$1_D$	1	$2^{14}$	1
$2_1$	$z$	1	$2^{14}$	1
$2_2$	$t$	2	$2^{13}$	1
$2_3$	$v$	4	$2^{12}$	1
$2_4$	$w$	8	$2^{11}$	1
$2_5$	$w_1$	16	$2^{10}$	1
$2_6$	$a$	16	$2^{10}$	1
$2_7$	$b$	32	$2^9$	1
$2_8$	$y$	32	$2^9$	1
$2_9$	$c$	64	$2^8$	1
$2_{10}$	$y_2$	64	$2^8$	1
$2_{11}$	$x_2y$	64	$2^8$	1
$2_{12}$	$wx_2y_2$	64	$2^8$	1
$2_{13}$	$ww_1ay_2$	64	$2^8$	1
$2_{14}$	$d$	128	$2^7$	1
$2_{15}$	$u$	128	$2^7$	1

Klasse	$\mathfrak{w}$	$ (\mathfrak{w})^D $	$ C_D(\mathfrak{w}) $	2P
$4_1$	$w_1a$	16	$2^{10}$	$2_1$
$4_2$	$x_1$	32	$2^9$	$2_1$
$4_3$	$wb$	32	$2^9$	$2_1$
$4_4$	$wy$	32	$2^9$	$2_2$
$4_5$	$x_1a$	32	$2^9$	$2_2$
$4_6$	$x_1y$	32	$2^9$	$2_1$
$4_7$	$x_2a$	32	$2^9$	$2_3$
$4_8$	$x_2b$	32	$2^9$	$2_3$
$4_9$	$(cy_2)^2$	32	$2^9$	$2_2$
$4_{10}$	$wx_1y$	32	$2^9$	$2_2$
$4_{11}$	$wx_2a$	32	$2^9$	$2_3$
$4_{12}$	$w_1x_2b$	32	$2^9$	$2_3$
$4_{13}$	$x_1x_2b$	32	$2^9$	$2_2$
$4_{14}$	$x_2$	64	$2^8$	$2_1$
$4_{15}$	$vc$	64	$2^8$	$2_1$
$4_{16}$	$wy_2$	64	$2^8$	$2_3$

Klasse	$\mathfrak{w}$	$ (\mathfrak{w})^D $	$ C_D(\mathfrak{w}) $	2P
4 <sub>17</sub>	$w_1y$	64	$2^8$	2 <sub>3</sub>
4 <sub>18</sub>	$w_1y_2$	64	$2^8$	2 <sub>3</sub>
4 <sub>19</sub>	$x_1b$	64	$2^8$	2 <sub>3</sub>
4 <sub>20</sub>	$x_1y_2$	64	$2^8$	2 <sub>2</sub>
4 <sub>21</sub>	$x_2y_2$	64	$2^8$	2 <sub>3</sub>
4 <sub>22</sub>	$ay_2$	64	$2^8$	2 <sub>2</sub>
4 <sub>23</sub>	$by$	64	$2^8$	2 <sub>3</sub>
4 <sub>24</sub>	$ww_1y_2$	64	$2^8$	2 <sub>2</sub>
4 <sub>25</sub>	$wx_1y_2$	64	$2^8$	2 <sub>3</sub>
4 <sub>26</sub>	$wx_2y$	64	$2^8$	2 <sub>2</sub>
4 <sub>27</sub>	$way_2$	64	$2^8$	2 <sub>3</sub>
4 <sub>28</sub>	$wby$	64	$2^8$	2 <sub>3</sub>
4 <sub>29</sub>	$w_1x_1y$	64	$2^8$	2 <sub>3</sub>
4 <sub>30</sub>	$w_1x_1y_2$	64	$2^8$	2 <sub>3</sub>
4 <sub>31</sub>	$w_1x_2y_2$	64	$2^8$	2 <sub>2</sub>
4 <sub>32</sub>	$w_1ay_2$	64	$2^8$	2 <sub>3</sub>
4 <sub>33</sub>	$x_2ay_2$	64	$2^8$	2 <sub>1</sub>
4 <sub>34</sub>	$ww_1x_2y_2$	64	$2^8$	2 <sub>3</sub>
4 <sub>35</sub>	$td$	128	$2^7$	2 <sub>1</sub>
4 <sub>36</sub>	$vu$	128	$2^7$	2 <sub>2</sub>
4 <sub>37</sub>	$x_1c$	128	$2^7$	2 <sub>4</sub>
4 <sub>38</sub>	$x_2c$	128	$2^7$	2 <sub>5</sub>
4 <sub>39</sub>	$x_2d$	128	$2^7$	2 <sub>4</sub>
4 <sub>40</sub>	$ad$	128	$2^7$	2 <sub>4</sub>
4 <sub>41</sub>	$tx_2c$	128	$2^7$	2 <sub>5</sub>
4 <sub>42</sub>	$x_1x_2d$	128	$2^7$	2 <sub>5</sub>
4 <sub>43</sub>	$vx_1x_2d$	128	$2^7$	2 <sub>5</sub>

Klasse	$\mathfrak{w}$	$ (\mathfrak{w})^D $	$ C_D(\mathfrak{w}) $	2P
4 <sub>44</sub>	$w_1u$	256	$2^6$	2 <sub>4</sub>
4 <sub>45</sub>	$x_1d$	256	$2^6$	2 <sub>5</sub>
4 <sub>46</sub>	$cy$	256	$2^6$	2 <sub>6</sub>
4 <sub>47</sub>	$y_2u$	256	$2^6$	2 <sub>8</sub>
4 <sub>48</sub>	$zy_2u$	256	$2^6$	2 <sub>8</sub>
4 <sub>49</sub>	$x_2bu$	256	$2^6$	2 <sub>6</sub>
4 <sub>50</sub>	$w_1x_2bu$	256	$2^6$	2 <sub>6</sub>
4 <sub>51</sub>	$dy_2$	512	$2^5$	2 <sub>7</sub>
4 <sub>52</sub>	$du$	512	$2^5$	2 <sub>9</sub>
4 <sub>53</sub>	$vdu$	512	$2^5$	2 <sub>9</sub>
8 <sub>1</sub>	$x_2cy$	256	$2^6$	4 <sub>1</sub>
8 <sub>2</sub>	$x_2u$	512	$2^5$	4 <sub>2</sub>
8 <sub>3</sub>	$bu$	512	$2^5$	4 <sub>5</sub>
8 <sub>4</sub>	$cy_2$	512	$2^5$	4 <sub>9</sub>
8 <sub>5</sub>	$dy$	512	$2^5$	4 <sub>8</sub>
8 <sub>6</sub>	$w_1y_2u$	512	$2^5$	4 <sub>4</sub>
8 <sub>7</sub>	$x_1cy_2$	512	$2^5$	4 <sub>13</sub>
8 <sub>8</sub>	$x_1dy$	512	$2^5$	4 <sub>12</sub>
8 <sub>9</sub>	$x_2dy_2$	512	$2^5$	4 <sub>3</sub>
8 <sub>10</sub>	$x_2y_2u$	512	$2^5$	4 <sub>6</sub>
8 <sub>11</sub>	$cdy_2$	512	$2^5$	4 <sub>7</sub>
8 <sub>12</sub>	$w_1x_2y_2u$	512	$2^5$	4 <sub>10</sub>
8 <sub>13</sub>	$x_1cdy_2$	512	$2^5$	4 <sub>11</sub>
8 <sub>14</sub>	$x_2du$	1024	$2^4$	4 <sub>37</sub>
16 <sub>1</sub>	$dy_2u$	1024	$2^4$	8 <sub>1</sub>
16 <sub>2</sub>	$(dy_2u)^3$	1024	$2^4$	8 <sub>1</sub>

**Beweis.** Mit Hilfe der Funktionen `LexLowestBaseConjugacyClassRepresentatives` und `InstallPrimePowermap` (siehe Unterabschnitt 3.5.2) bestimmt MAGMA für die Permutationsgruppe  $D = S = \pi_S(S) \leq S_{512}$  das oben angegebene Repräsentantensystem inklusive 2-Potenzabbildung in knapp 24 CPU-Minuten<sup>3</sup>.  $\square$

Indem wir die obigen Worte sowohl in  $D$  als auch in  $\mu(D)$  ausmultiplizieren, produzieren wir die Konjugiertenklassenvertretersequenzen  $ccs_1$  und  $ccs_2$ , welche zusammen mit den Charaktertafeln von  $H$ ,  $D$ ,  $E_\Phi$  und  $\mu(D)$  von der Funktion `RestrictionsOnIsomorphicSubgroups` (vergleiche Unterabschnitt 4.3.1) als Aufrufparameter verlangt werden.

Von den insgesamt 49 irreduziblen  $\mathbb{C}$ -Charakteren der Gruppe  $H$  haben genau fünf Stück die Involution  $z$  nicht im Kern, nämlich<sup>4</sup>  $\chi_{45}$ ,  $\chi_{46}$  und  $\chi_{47}$  vom Grad 128 sowie  $\chi_{48}$  und  $\chi_{49}$  vom Grad 192. Aus der Menge ebendieser Charaktere ist deshalb der Sollkonstituent  $\xi$  zu wählen,

<sup>3</sup>Messgrundlage war erneut ein PC mit 450 MHz Pentium-III-Prozessor und 512 MB Arbeitsspeicher.

<sup>4</sup>Die benutzte Nummerierung ist willkürlich und dient allein der notationellen Unterscheidung.

wenn mittels der Funktion `SearchCompatiblePairs` (siehe Unterabschnitt 4.3.1) nach den über  $D$  kompatiblen Paaren  $(\chi, \vartheta) \in \Pi := \underline{\text{Char}}_{\mathbb{C}}^{\sharp}(H) \times \underline{\text{Char}}_{\mathbb{C}}(E_{\Phi})$  minimalen Grades  $d$  gesucht wird.

Leider stößt eine solche, relativ eng an den Originalinstruktionen des Michler-Algorithmus orientierte Rechnung unabhängig von der Wahl des Sollkonstituenten  $\xi$  auf unvorhersehbare Schwierigkeiten:

**Fall 1:** Sei  $\xi := \chi_j$  mit  $j \in \{45, 46, 47\}$ . Dann besteht die Menge  $\Pi_{H,\xi}^{\leq 274}$  jeweils aus exakt zwei kompatiblen Paaren vom Grad 274, als da sind

$$(\chi_0 + \chi_j, \vartheta_0 + \vartheta_1) \quad \text{und} \quad (\chi_0 + \chi_j, \vartheta_0 + \vartheta_2),$$

wobei  $\vartheta_1$  die Summe der beiden irreduziblen Charaktere von  $E_{\Phi}$  vom Grad 16 bezeichnet,  $\vartheta_2 \in \text{Irr}_{\mathbb{C}}(E_{\Phi})$  vom Grad 32 ist und die gemeinsamen Summanden  $\chi_0, \vartheta_0$  gradmäßig wie folgt in irreduzible Bestandteile zerfallen (treue Konstituenten fett gedruckt):

$$\begin{aligned} \chi_0 &= 4 + 10 + 12 + 60_1 + 60_2, \\ \vartheta_0 &= \mathbb{1}_{E_{\Phi}} + 3 + 4 + 6_1 + 12_1 + 12_2 + 12_3 + \mathbf{96_1} + \mathbf{96_2}. \end{aligned}$$

Für alle  $j \in \{45, 46, 47\}$  ergibt sich als gemeinsame Restriktion der Komponenten beider Paare auf  $D$  derselbe multiplizitätenfreie Charakter, nämlich

$$\delta = \mathbb{1}_D + 1 + 2_1 + 2_2 + 4_1 + \dots + 4_7 + 8_1 + 8_2 + 16_1 + 16_2 + 32_1 + 32_2 + \mathbf{64_1} + \mathbf{64_2}.$$

Um aus den kompatiblen Partnern korrespondierende Matrixdarstellungen über einem endlichen Primkörper  $\text{GF}(p)$  zu bauen, können wir allerdings nur für die Paare mit dem überall rationalen Sollkonstituenten  $\chi_{47}$  die minimale Charakteristik  $p = 7$  wählen. Die Charaktere  $\chi_{45}$  und  $\chi_{46}$  sind hingegen algebraisch konjugiert und nehmen auf Elementen der Ordnung 24 den Wert  $\pm\sqrt{6}$  an, welcher erst in  $\text{GF}(19)$  mit  $5 + 19\mathbb{Z}$  ein vollwertiges Pendant hat.

Laut Lemma 2.2.5 wäre also die Anzahl der zu untersuchenden Amalgame gleich

- $6^3 = 216$  für das Paar  $(\chi_0 + \chi_{47}, \vartheta_0 + \vartheta_2)$ ,
- $6^4 = 1296$  für das Paar  $(\chi_0 + \chi_{47}, \vartheta_0 + \vartheta_1)$ ,
- $18^3 = 5832$  für die Paare  $(\chi_0 + \chi_j, \vartheta_0 + \vartheta_2)$ ,  $j \in \{45, 46\}$  und
- $18^4 = 104976$  für die Paare  $(\chi_0 + \chi_j, \vartheta_0 + \vartheta_1)$ ,  $j \in \{45, 46\}$ .

**Fall 2:** Sei  $\xi := \chi_{48}$ . Dann besteht die Menge  $\Pi_{H,\xi}^{\leq 378}$  aus exakt zwei kompatiblen Paaren vom Grad 378, als da sind

$$(\chi_0 + \chi_6 + \chi_{48}, \vartheta_0 + \vartheta_6) \quad \text{und} \quad (\chi_0 + \overline{\chi_6} + \chi_{48}, \vartheta_0 + \overline{\vartheta_6}),$$

wobei  $\chi_6$  bzw.  $\vartheta_6$  die durch  $\chi_6(dy_2u) = \vartheta_6(dy_2u) = 2i$ ,  $i^2 = -1$ , eindeutig festgelegten irreduziblen Charaktere von  $H$  bzw.  $E_{\Phi}$  vom Grad 6 bezeichnen und die gemeinsamen Summanden  $\chi_0, \vartheta_0$  gradmäßig wie folgt in rationale irreduzible Bestandteile zerfallen:

$$\begin{aligned} \chi_0 &= 60_3 + 120, \\ \vartheta_0 &= 12_4 + 24 + 48 + \mathbf{96_1} + \mathbf{96_3} + \mathbf{96_4}. \end{aligned}$$

Ohne Einschränkung dürften wir uns in diesem Fall auf die Betrachtung des ersten Paares spezialisieren, führt das zweite doch lediglich zu einer dualen Darstellung derselben Matrixgruppe. Unglücklicherweise ist aber die gemeinsame Restriktion der beiden Komponenten auf  $D$  nicht multiplizitätenfrei, sondern enthält einen ihrer 14 verschiedenen irreduziblen Konstituenten doppelt.

Zudem zwingt uns die Beteiligung von  $\chi_6$  respektive  $\vartheta_6$ , über einem Primkörper  $\text{GF}(p)$  mit 4-ter Einheitswurzel zu arbeiten. Diesbezüglich wäre  $p = 13$  die kleinste in Frage kommende Charakteristik, welche das Produkt  $|H||E_\Phi|$  nicht teilt.

Gemäß J. G. Thompson [43] hätten wir dann  $\geq 12^5 = 248832$  Amalgame zu testen!

**Fall 3:** Sei  $\xi := \chi_{49}$ . Dann ist die Menge  $\Pi_{H,\xi}^{\leq 400}$  leer.

Angesichts des ziemlich unwegsamen Geländes, das uns über jedem Körper von zu  $|H||E_\Phi|$  teilerfremder Charakteristik erwartet, scheint eine modulare Ausweichroute in der Tat noch die bestmögliche Lösung zu sein. Obwohl erst  $\text{GF}(5^2)$  ein Zerfällungskörper für die Gruppe  $E_\Phi$  ist (benötigt wird hier eine 3-te Einheitswurzel), fiel die Wahl auf Charakteristik  $p = 5$ ; diese Primzahl geht in  $|E_\Phi|$  überhaupt nicht und in  $|H|$  nur zur ersten Potenz auf.

#### 5.4.2 Experiment B: 5-modulare Darstellungstheorie

Statt der Charaktertafeln von  $H$ ,  $E_\Phi$ ,  $D$  und  $\mu(D)$  gilt es jetzt, ein Repräsentantensystem für die irreduziblen Moduln dieser Gruppen über  $\mathbb{F} := \text{GF}(5)$  bzw. über  $\text{GF}(5^2)$  zu finden.

Weil  $\mathbb{F}$  ein Zerfällungskörper für  $H$  ist, entspricht die Anzahl der paarweise nicht-isomorphen irreduziblen  $\mathbb{F}H$ -Moduln gerade der Anzahl der  $5'$ -Konjugiertenklassen von  $H$ . Wie man zum Beispiel anhand der für Experiment A ermittelten gewöhnlichen Charaktertafel von  $H$  leicht bestätigt, existieren demnach 44 paarweise nicht-isomorphe irreduzible  $\mathbb{F}H$ -Moduln. Fast jeden davon trifft wenigstens einmal, wer die MAGMA-Implementierung von R. A. Parkers MEAT-AXE [34] sukzessive auf

1. den Permutationsmodul von  $H$  über  $\mathbb{F}$  der Dimension 2048; darin enthalten sind unter anderem genau ein (nicht-treuer) Konstituent  $W_1$  der Dimension 12 sowie ein treuer Konstituent  $W_2$  der Dimension 64, welcher mit Vielfachheit 3 auftritt.
2. das Tensorquadrat  $W_1 \otimes W_1$  und
3. das Tensorquadrat  $W_2 \otimes W_2$

anwendet. Dies liefert schon 43 Zielobjekte. Das letzte, ein Modul der Dimension 10, entsteht durch Abschluss des berechneten Modulsystems gegenüber Tensorierung mit dem Signumscharakter.

Wegen  $\text{ggT}(|E_\Phi|, 5) = 1$  besitzt  $E_\Phi$  genauso viele paarweise nicht-isomorphe irreduzible Moduln über  $\text{GF}(5^2)$  wie irreduzible Charaktere über  $\mathbb{C}$ , nämlich 53 — man vergleiche mit der für Experiment A bestimmten Tafel. Um die Moduln aufzuspüren, zerlegen wir nacheinander

1. den Permutationsmodul  $P$  von  $E_\Phi$  über  $\text{GF}(5^2)$  und
2. das symmetrische Tensorquadrat eines der vier in  $P$  vorkommenden treuen Konstituenten der Dimension 96.

Zum kompletten Vertretersystem fehlt im Anschluss an diese Prozedur wiederum exakt ein einziger Modul, diesmal der Dimension 24. Die Lücke lässt sich füllen, indem wir willkürlich einen der schon bekannten Moduln selbiger Dimension auswählen und die irreduziblen Konstituenten seines Tensorquadrats analysieren.

**Bemerkung:** Abgesehen von zwei nicht-treuen Ausnahmen der Dimension 8, sind übrigens alle irreduziblen  $E_\Phi$ -Moduln bereits über dem Körper  $\mathbb{F}$  absolut irreduzibel.

Repräsentantensysteme für die irreduziblen  $\mathbb{F}D$ - bzw.  $\mathbb{F}\mu(D)$ -Moduln zu konstruieren ist nun nicht weiter schwierig: Man restringiere einfach jeden der vorliegenden Vertretermoduln für  $H$  bzw.  $E_\Phi$  auf die entsprechende Untergruppe, zerlege die Restriktionen in ihre irreduziblen Bestandteile und sammle paarweise nicht-isomorphe Konstituenten. Elementare Darstellungstheorie gewährleistet, dass die so erhaltenen Modulmengen tatsächlich aus jeder Isomorphieklasse einen Vertreter zu bieten haben.

Damit stehen uns sämtliche von der Funktion `RestrictionsOnIsomorphicSubgroups_MOD` (siehe Unterabschnitt 4.3.1) verlangten Eingabedaten zur Verfügung; die Konjugiertenklassenrepräsentantensequenzen  $ccs_1$  und  $ccs_2$  können wir unverändert aus Experiment A übernehmen.

#### Satz 5.4.2

*Es bezeichne  $\Pi$  die Menge der über  $D$  kompatiblen Paare  $(M, N)$  von treuen multiplizitätenfreien  $\text{GF}(5^2)H$ -Moduln  $M$  und treuen  $\text{GF}(5^2)E_\Phi$ -Moduln  $N$ .*

*Dann enthält  $\Pi$  genau ein Element  $(M_{\min}, N_{\min})$  minimaler Dimension 133, dessen Komponenten halbeinfach sind und dimensionsmäßig wie folgt in irreduzible Konstituenten zerfallen:*

$$\begin{aligned} M_{\min} &= 3 \oplus 6 \oplus 60 \oplus \mathbf{64} , \\ N_{\min} &= 3 \oplus 6 \oplus 12 \oplus 16 \oplus \mathbf{96} . \end{aligned}$$

*Die gemeinsame Restriktion  $V$  von  $M_{\min}$  und  $N_{\min}$  auf  $D$  ist multiplizitätenfrei, ebenfalls halbeinfach und zerfällt dimensionsmäßig in die folgenden neun irreduziblen Bestandteile:*

$$V = 1 \oplus 2_1 \oplus 2_2 \oplus 4_1 \oplus 4_2 \oplus 8 \oplus 16 \oplus 32 \oplus \mathbf{64} .$$

**Beweis.** Unter den 44 irreduziblen  $\text{GF}(5^2)H$ -Moduln sind exakt vier, auf denen die Involution  $z$  treu operiert, nämlich  $M_{35}$  und  $M_{36}$  der Dimension 64 sowie  $M_{43}$  und  $M_{44}$  der Dimension 128. Die erste Komponente eines jeden Paares  $(M, N) \in \Pi$  muss daher einen Konstituenten  $Y$  aus der Menge  $\{M_j \mid j = 35, 36, 43, 44\}$  beziehen.

MAGMA berechnet mit Hilfe der Funktion `SearchCompatiblePairs_MOD` (vergleiche Unterabschnitt 4.3.1), dass

$$\Pi_{H,Y}^{\leq 133} = \emptyset \quad \text{für } Y = M_j, j \in \{36, 43, 44\} ,$$

und dass

$$\Pi_{H,M_{35}}^{\leq 133} = \{(M_{\min}, N_{\min})\} ,$$

wobei die Komponenten  $M_{\min}$  und  $N_{\min}$  bzw. ihre gemeinsame Restriktion  $V$  auf die Gruppe  $D$  jeweils in irreduzible Konstituenten der behaupteten Dimensionen zerfallen.

Wegen  $\text{ggT}(|E_\Phi|, 5) = 1$  sind  $N_{\min}$  und  $V$  nach dem Satz von Maschke halbeinfach. Zu zeigen bleibt deshalb lediglich die Halbeinfachheit des  $H$ -Moduls  $M_{\min}$ .

Da **64** der einzige treue und **60** der einzige Konstituent vom 5-Defekt 0 von  $M_{\min}$  ist, spalten diese beiden Submoduln garantiert direkt ab. Ferner gilt  $3 \downarrow_D = 1 \oplus 2_1$ , weil  $\text{ggT}(|D|, 5) = 1$ .

Angenommen, die Konstituenten 3 und 6 von  $M_{\min}$  liegen im selben 5-Block von  $H$ . Dann müsste 6 insbesondere in der  $H$ -projektiven Hülle von 1, also in  $1 \uparrow^H$  auftreten. Mit MAGMA verifiziert man jedoch sofort, dass

$$1 \uparrow^H = 5 \oplus \begin{pmatrix} 3 \\ 1_1 + 3_1 \\ 3 \end{pmatrix} .$$

Hieraus folgt die Behauptung.  $\square$

### 5.4.3 Amalgamierung und 2-Sylowuntergruppentest

Laut Satz 5.4.2 besitzt der Modul  $N_{\min}$  keinen irreduziblen Konstituenten der Dimension 8. Aufgrund der Bemerkung im vorangegangenen Unterabschnitt können wir die Schritte 4b und 4c des Michler-Algorithmus demnach problemlos über dem Primkörper  $\mathbb{F} = \text{GF}(5)$  ausführen.

#### $\square$ Schritt 4b

Aus den Moduln  $M := M_{\min}$  und  $N := N_{\min}$  gewinnt MAGMA binnen Sekunden die korrespondierenden  $\mathbb{F}$ -Darstellungen  $\mathfrak{M} : H \rightarrow \text{GL}_{133}(5)$  und  $\mathfrak{N} : E_{\Phi} \rightarrow \text{GL}_{133}(5)$ . Das Bild  $\mathfrak{M}(H)$  ist gemäß Satz 5.1.10 durch die Angabe der Matrizen  $\mathfrak{M}(k)$  und  $\mathfrak{M}(f)$  eindeutig bestimmt; beide sind Anhang A zu entnehmen. Dort findet der Leser auch die Matrix  $\mathfrak{N}(t_0)$  sowie eine Transformationsmatrix  $T \in L := \text{GL}_{133}(5)$  mit

$$T^{-1} \mathfrak{N}(\mu(x)) T = \mathfrak{M}(x) \quad \text{für alle } x \in D .$$

Das Bild  $\mathfrak{N}(E_{\Phi})$  ist anhand dieser Daten vollständig rekonstruierbar.

Weil die gemeinsame Restriktion  $V$  von  $M$  und  $N$  auf die Gruppe  $D$  keinerlei Multiplizität aufweist, ist  $\mathbf{C}_L(\mathfrak{M}(D))$  nach dem Lemma von Schur ein direktes Produkt zyklischer Gruppen. Speziell degenerieren die  $\mathbf{C}_L(\mathfrak{M}(H))$ - $\mathbf{C}_L(\mathfrak{N}(E_{\Phi})^T)$ -Doppelnebenklassen in  $\mathbf{C}_L(\mathfrak{M}(D))$  somit zu gewöhnlichen Nebenklassen und mit Blick auf das Zerlegungsmuster von  $V$  in Satz 5.4.2 erkennen wir die Menge der Diagonalmatrizen

$$C_j := \text{Diag}(j, 1, \dots, 1) \in L, \quad j \in \mathbb{F}^*$$

als Vertretersystem dieser Nebenklassen.

#### $\square$ Schritt 4c

Im Rahmen des 2-Sylowuntergruppentests ergibt sich folgende Situation:

- Die Gruppe  $G_2 := \langle \mathfrak{M}(H), \mathfrak{N}(E_{\Phi})^{TC_2} \rangle$  enthält mit  $\mathfrak{M}(f) \mathfrak{N}(t_0)^{TC_2} \mathfrak{M}(u)$  eine Matrix der Ordnung

$$2^5 \cdot 3 \cdot 5 \cdot 13 \cdot 313 \cdot 19531 .$$

Eine 2-Sylowuntergruppe von  $G_2$  kann daher niemals isomorph zu  $S$  sein, denn in  $S$  existiert kein Element der Ordnung 32.

- Die Gruppe  $G_3 := \langle \mathfrak{M}(H), \mathfrak{N}(E_\Phi)^{TC_3} \rangle$  enthält mit  $\mathfrak{M}(f)\mathfrak{N}(t_0)^{TC_3}\mathfrak{M}(y_2)$  eine Matrix der Ordnung

$$2^6 \cdot 3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 67 \cdot 71 \cdot 313 \cdot 521 \cdot 5281 \cdot 11489 \cdot 12207031 .$$

Eine 2-Sylowuntergruppe von  $G_4$  kann daher niemals isomorph zu  $S$  sein, denn in  $S$  existiert kein Element der Ordnung 64.

- Die Gruppe  $G_4 := \langle \mathfrak{M}(H), \mathfrak{N}(E_\Phi)^{TC_4} \rangle$  enthält mit  $\mathfrak{M}(f)^4\mathfrak{N}(t_0)^{TC_4}$  eine Matrix der Ordnung

$$2^5 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 71 \cdot 313 \cdot 521 .$$

Eine 2-Sylowuntergruppe von  $G_4$  kann daher niemals isomorph zu  $S$  sein, denn in  $S$  existiert kein Element der Ordnung 32.

Allein die Gruppe

$$G := G_1 := \langle \mathfrak{M}(H), \mathfrak{N}(E_\Phi)^{TC_1} \rangle = \langle \mathfrak{M}(H), \mathfrak{N}(E_\Phi)^T \rangle = \langle \mathfrak{M}(k), \mathfrak{M}(f), \mathfrak{N}(t_0)^T \rangle$$

besteht den Test und schafft es so, in Schritt 5 des Michler-Algorithmus zu gelangen.

## 5.5 Das Endergebnis: 593775 Punkte

Gesucht ist eine treue Permutationsdarstellung der Matrixgruppe  $G$ . Während  $\mathfrak{N}(t_0)$  durch die Konjugation mit  $T$  eine dichte Matrix wird, teilen alle Elemente von  $\mathfrak{M}(H)$  die charakteristische Blockdiagonalstruktur der beiden Erzeuger  $\mathfrak{M}(k)$  und  $\mathfrak{M}(f)$ . Der Stabilisator

$$H_0 := \text{Stab}_G(U)$$

des von den ersten drei kanonischen Basisvektoren erzeugten Untervektorraums  $U \leq \mathbb{F}^{133}$  ist infolgedessen eine echte Untergruppe in  $G$ , die  $\mathfrak{M}(H)$  umfasst. Diese Rahmenbedingungen sind quasi prädestiniert für einen Einsatz des Algorithmus von G. Cooperman, L. Finkelstein, M. Tselman und B. York [9].

Nachdem die MAGMA-Implementierung dieses Verfahrens — die Funktion `OrbitAction` — mit Hinweis auf beschränkte Hauptspeicherressourcen kapitulierte, wurde auf eine C-Version zurückgegriffen, die K. Waki während seines Gastaufenthaltes am Institut für Experimentelle Mathematik programmiert und dem Autor dankenswerterweise zur Verfügung gestellt hat. In rund 13,8 CPU-Stunden<sup>5</sup> konnte damit eine Permutationsdarstellung

$$\pi_G : G \rightarrow S_{593775}$$

samt Schreiervektor für den Orbit  $(U)^G$  produziert werden.

### Lemma 5.5.1

Die Permutationsdarstellung  $\pi_G$  von  $G$  ist treu; insbesondere gilt:

$$|G| = |\pi_G(G)| = 145926144000 .$$

**Beweis.** MAGMA mag nicht in der Lage gewesen sein, den Homomorphismus  $\pi_G$  selber zu konstruieren, bewerkstelligt Rechnungen in  $\pi_G(G)$  aber einwandfrei, sobald die mit

---

<sup>5</sup>auf einer RISC 6000 Model 590 Workstation mit 1 GB Arbeitsspeicher



Hilfe von Wakis C-Programm `vs_orbit` gefundenen Bilder

$$\mathfrak{k} := \pi_G(\mathfrak{M}(k)), \quad \mathfrak{f} := \pi_G(\mathfrak{M}(f)) \quad \text{und} \quad \mathfrak{t}_0 := \pi_G(\mathfrak{M}(t_0)^T)$$

der Erzeuger von  $G$  in das System eingespeist werden. Unter anderem bestätigt MAGMA, dass  $|\pi_G(G)|$  wie behauptet der Ordnung der Rudvalis-Gruppe entspricht und dass

$$|\pi_G(\mathfrak{M}(H))| = |\langle \mathfrak{k}, \mathfrak{f} \rangle| = 245760 = |\mathfrak{M}(H)|.$$

Folglich ist  $\pi_G$  treu auf  $\mathfrak{M}(H) \leq H_0$ . Wegen  $\text{Kern } \pi_G \leq H_0$  reicht es also, die Inklusion  $\mathfrak{M}(H) \geq H_0$  respektive die Gleichheit

$$\mathfrak{M}(H) = H_0 = \text{Stab}_G(U) \tag{P}$$

nachzuweisen.

Ohne Einschränkung identifizieren wir fortan  $\pi_G(\mathfrak{M}(H))$  mit  $H$  und wenden den auf Ideen von C. C. Sims [unveröffentlicht] basierenden und von H. W. Gollan [15] entwickelten „Doppelnebenklassentrick“ an: Dieser Algorithmus liefert zwei Klassen von Relationen in den drei Erzeugern  $\mathfrak{k}$ ,  $\mathfrak{f}$  und  $\mathfrak{t}_0$  von  $\pi_G(G)$ , deren Gültigkeit äquivalent ist zur Aussage

$$H = \text{Stab}_{\pi_G(G)}(1).$$

Die Verifikation der entsprechenden Relationen in den Erzeugern  $\mathfrak{M}(k)$ ,  $\mathfrak{M}(f)$  und  $\mathfrak{M}(t_0)^T$  von  $G$  würde mithin (P) implizieren.

Sei  $\Omega := \{1, 2, \dots, 593775\}$  die Menge der Punkte, auf denen die Gruppe  $\pi_G(G)$  operiert. Per Identifikation gilt  $H = \langle k, f \rangle = \langle \mathfrak{k}, \mathfrak{f} \rangle \leq \pi_G(G)$  und  $\mathfrak{t}_0 \notin H$ . Darüber hinaus ermittelt MAGMA (siehe Anhang B.1 für explizite Daten)

- ein Vertretersystem  $\Gamma := \{\gamma_1, \gamma_2, \dots, \gamma_{22}\}$  der  $H$ -Orbits auf  $\Omega = (1)^{\pi_G(G)}$ ;
- zu jedem Index  $i \in \{1, 2, \dots, 22\}$  eine Permutation  $r_i \in \pi_G(G)$  mit  $1_i^r = \gamma_i$ .

Die Menge  $\{r_1, r_2, \dots, r_{22}\}$  ist ein Repräsentantensystem der  $H$ - $H$ -Doppelnebenklassen in  $\pi_G(G)$  und zu jedem Punkt  $\omega \in \Omega$  existiert genau ein  $i_\omega \in \{1, 2, \dots, 22\}$  mit  $\omega \in (\gamma_{i_\omega})^H$ . Für  $\omega \in \Omega$  bezeichne  $h_\omega \in H$  eine fixierte Permutation, die den Orbitanfangspunkt  $\gamma_{i_\omega}$  auf  $\omega$  wirft.

Der Doppelnebenklassentrick setzt sich aus zwei Teilen zusammen:

**Schritt 1:** Prüfe, ob

$$Hr_iH \subseteq \bigcup_{\omega \in (\gamma_{i_\omega})^H} Hr_ih_\omega \quad \text{für alle } 1 \leq i \leq 22.$$

Sofern zu jedem  $i \in \{1, 2, \dots, 22\}$  Erzeuger  $y_{i,1}, y_{i,2}, \dots, y_{i,\ell_i}$  des Stabilisators  $\text{Stab}_H(\gamma_i)$  berechnet wurden, ist diese Bedingung laut Bemerkung 3.1.4 in [15] äquivalent zu

$$y_{i,j}^{r_i^{-1}} \in H \quad \text{für alle } 1 \leq i \leq 22 \text{ und alle } 1 \leq j \leq \ell_i.$$

**Schritt 2:** Prüfe, ob jede Rechtsnebenklasse

$$Hr_ih_\omega\mathfrak{t}_0, \quad 1 \leq i \leq 22, \quad \omega \in (\gamma_i)^H,$$

in einer Doppelnebenklasse  $Hr_jH$ ,  $1 \leq j \leq 22$ , enthalten ist.

Nach Bemerkung 3.1.2 in [15] genügt es für  $K := H \cap H^{\mathfrak{t}_0^{-1}}$  und ein Vertreter-system  $\Lambda$  der  $K$ -Orbits auf  $\Omega$  zu zeigen, dass für alle Indices  $i \in \{1, 2, \dots, 22\}$  und alle Repräsentanten  $\lambda \in \Lambda$  gilt:

$$\exists j \in \{1, 2, \dots, 22\}, h(i, \lambda) \in H : Hr_i h_\lambda \mathfrak{t}_0 = Hr_j h(i, \lambda) .$$

Führen wir unter MAGMA beide Tests in  $\pi_G(G)$  durch, so erhalten wir in jedem Fall eine positive Antwort. Aus Schritt 1 ergeben sich insgesamt 54 nicht-triviale Relationen der Form

$$y_{i,j}^{r_i^{-1}} = v_{i,j}(k, f) , \quad (\text{Q})$$

die in Anhang B.2 zu begutachten sind. Ferner zerfällt  $\Omega$  in 172  $K$ -Orbits und mit Ausnahme von  $(1)^K = \{1\}$  deckt Schritt 2 für jeden dieser Orbits eine nicht-triviale Relation der Gestalt

$$r_i h_\lambda \mathfrak{t}_0 (r_j h(i, \lambda))^{-1} = w_{i,\lambda}(k, f) \quad (\text{R})$$

auf, welche der Leser alle in Anhang B.3 wieder findet. Wesentlich ist jedoch, dass auch die in den Erzeugern von  $G$  formulierten Relationen (Q) und (R) durchwegs erfüllt werden.

Es folgt  $\mathfrak{M}(H) = H_0$  und somit die Behauptung.  $\square$

Lemma 5.5.1 erlaubt uns, die Matrixgruppe  $G$  fortan mit ihrem Bild unter der Permutationsdarstellung  $\pi_G$  zu identifizieren. Diese Sichtweise ist der entscheidende methodische Schlüssel für die abschließende Analyse des Isomphietyps von  $G$ .

### Satz 5.5.2

Mit den bisher eingeführten Bezeichnungen gilt:

$$G = \langle k, f, \mathfrak{t}_0 \rangle \cong \text{Ru} .$$

Die unten abgedruckte Tabelle beschreibt ein Repräsentantensystem für die 36 Konjugiertenklassen von  $G$ , bestehend aus den Vertretern  $\mathfrak{w}$  mit lexikographisch kleinster Basis bezüglich der Erzeugermenge von  $G$ , sowie die  $p$ -Potenzabbildungen für sämtliche Primteiler  $p$  von  $|G|$ :

Klasse	$\mathfrak{w}$	$ (\mathfrak{w})^D $	$ \mathbf{C}_D(\mathfrak{w}) $	2P	3P	5P	7P	13P	29P
1	1	1	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	1	1	1	1	1	1
$2_1$	$k^2$	593775	$2^{14} \cdot 3 \cdot 5$	1	$2_1$	$2_1$	$2_1$	$2_1$	$2_1$
$2_2$	$(f\mathfrak{t}_0)^5$	1252800	$2^8 \cdot 5 \cdot 7 \cdot 13$	1	$2_2$	$2_2$	$2_2$	$2_2$	$2_2$
3	$\mathfrak{t}_0$	67558400	$2^4 \cdot 3^3 \cdot 5$	3	1	3	3	3	3
$4_1$	$(kf)^2$	19000800	$2^9 \cdot 3 \cdot 5$	$2_1$	$4_1$	$4_1$	$4_1$	$4_1$	$4_1$
$4_2$	$(f\mathfrak{t}_0)^3$	38001600	$2^8 \cdot 3 \cdot 5$	$2_1$	$4_2$	$4_2$	$4_2$	$4_2$	$4_2$
$4_3$	$(kft_0)^4$	142506000	$2^{10}$	$2_1$	$4_3$	$4_3$	$4_3$	$4_3$	$4_3$
$4_4$	$k$	285012000	$2^9$	$2_1$	$4_4$	$4_4$	$4_4$	$4_4$	$4_4$
$5_1$	$f$	145926144	$2^3 \cdot 5^3$	$5_1$	$5_1$	1	$5_1$	$5_1$	$5_1$
$5_2$	$(f\mathfrak{t}_0)^2$	486420480	$2^2 \cdot 3 \cdot 5^2$	$5_2$	$5_2$	1	$5_2$	$5_2$	$5_2$
6	$kf^2$	3040128000	$2^4 \cdot 3$	3	$2_1$	6	6	6	6
7	$(k\mathfrak{t}_0 f)^2$	5211648000	$2^2 \cdot 7$	7	7	7	1	7	7
$8_1$	$kf$	1520064000	$2^5 \cdot 3$	$4_1$	$8_1$	$8_1$	$8_1$	$8_1$	$8_1$
$8_2$	$(kft_0)^2$	2280096000	$2^6$	$4_3$	$8_2$	$8_2$	$8_2$	$8_2$	$8_2$
$8_3$	$k^2 f \mathfrak{t}_0$	4560192000	$2^5$	$4_4$	$8_3$	$8_3$	$8_3$	$8_3$	$8_3$

Klasse	$\mathfrak{w}$	$ (\mathfrak{w})^D $	$ C_D(\mathfrak{w}) $	2P	3P	5P	7P	13P	29P
$10_1$	$k^2 f^2$	3648153600	$2^3 \cdot 5$	$5_1$	$10_1$	$2_1$	$10_1$	$10_1$	$10_1$
$10_2$	$f t_0$	7296307200	$2^2 \cdot 5$	$5_2$	$10_2$	$2_2$	$10_2$	$10_2$	$10_2$
$12_1$	$(f^2 t_0)^2$	6080256000	$2^3 \cdot 3$	6	$4_1$	$12_1$	$12_1$	$12_1$	$12_1$
$12_2$	$f t_0^2$	12160512000	$2^2 \cdot 3$	6	$4_2$	$12_2$	$12_2$	$12_2$	$12_2$
13	$(k f^2 t_0)^2$	2806272000	$2^2 \cdot 13$	13	13	13	13	1	13
$14_1$	$k t_0 f$	5211648000	$2^2 \cdot 7$	7	$14_2$	$14_3$	$2_2$	$14_1$	$14_1$
$14_2$	$(k t_0 f)^3$	5211648000	$2^2 \cdot 7$	7	$14_3$	$14_1$	$2_2$	$14_2$	$14_2$
$14_3$	$(k t_0 f)^5$	5211648000	$2^2 \cdot 7$	7	$14_1$	$14_2$	$2_2$	$14_3$	$14_3$
15	$f t_0 f t_0^2$	9728409600	$3 \cdot 5$	15	$5_2$	3	15	15	15
$16_1$	$k f t_0$	9120384000	$2^4$	$8_2$	$16_2$	$16_1$	$16_2$	$16_1$	$16_1$
$16_2$	$(k f t_0)^3$	9120384000	$2^4$	$8_2$	$16_1$	$16_2$	$16_1$	$16_2$	$16_2$
$20_1$	$k t_0 f t_0$	7296307200	$2^2 \cdot 5$	$10_1$	$20_2$	$4_2$	$20_2$	$20_2$	$20_1$
$20_2$	$(k t_0 f t_0)^3$	7296307200	$2^2 \cdot 5$	$10_1$	$20_1$	$4_2$	$20_1$	$20_1$	$20_2$
$20_3$	$k f t_0 f t_0$	7296307200	$2^2 \cdot 5$	$10_1$	$20_3$	$4_1$	$20_3$	$20_3$	$20_3$
$24_1$	$f^2 t_0$	6080256000	$2^3 \cdot 3$	$12_1$	$8_1$	$24_1$	$24_2$	$24_2$	$24_1$
$24_2$	$(f^2 t_0)^7$	6080256000	$2^3 \cdot 3$	$12_1$	$8_1$	$24_2$	$24_1$	$24_1$	$24_2$
$26_1$	$k f^2 t_0$	2806272000	$2^2 \cdot 13$	13	$26_2$	$26_1$	$26_3$	$2_2$	$26_2$
$26_2$	$(k f^2 t_0)^3$	2806272000	$2^2 \cdot 13$	13	$26_3$	$26_2$	$26_1$	$2_2$	$26_3$
$26_3$	$(k f^2 t_0)^7$	2806272000	$2^2 \cdot 13$	13	$26_1$	$26_3$	$26_2$	$2_2$	$26_1$
$29_1$	$k f k t_0 f t_0$	5031936000	29	$29_2$	$29_2$	$29_1$	$29_1$	$29_1$	1
$29_2$	$(k f k t_0 f t_0)^2$	5031936000	29	$29_1$	$29_1$	$29_2$	$29_2$	$29_2$	1

**Beweis.** Mit Hilfe der Funktionen `LexLowestBaseConjugacyClassRepresentatives` und `InstallPrimePowermap` (vergleiche Unterabschnitt 3.5.2) bestimmt MAGMA für die Permutationsgruppe  $G \leq S_{593775}$  das oben angegebene Repräsentantensystem inklusive Primpotenzabbildungen in 20,8 CPU-Stunden<sup>6</sup>.

Da der hohe Permutationsgrad von  $G$  den direkten Einsatz des Dixon-Schneider-Algorithmus verbietet, ist die Berechnung einer konkreten Charaktertafel von  $G$  nur in Etappen zu realisieren:

1. Ermittlung des Gollan-Ostermann-Vektors  $GO_H(\mathfrak{w})$  für jeden Konjugiertenklassenvertreter  $\mathfrak{w}$  unter MAGMA in insgesamt 1,7 CPU-Stunden<sup>7</sup>.
2. Zerlegung des Permutationscharakters von  $\pi_G$  in irreduzible Konstituenten gemäß G. O. Michler und M. Weller [33] in 1,8 CPU-Stunden<sup>8</sup>.  
Es stellt sich heraus, dass  $\pi_G$  nicht multiplizitätenfrei ist und neben  $\mathbb{1}_G$  noch exakt 15 weitere paarweise verschiedene irreduzible Konstituenten enthält. Bezüglich der Tafel in Anhang C sind dies die Charaktere  $\chi_5$ – $\chi_7$  ( $\chi_6$  doppelt),  $\chi_{10}$ – $\chi_{16}$  ( $\chi_{14}$  doppelt),  $\chi_{20}$ ,  $\chi_{22}$ ,  $\chi_{23}$ ,  $\chi_{26}$  und  $\chi_{32}$ .
3. Durchlaufen der Schritte 2–5 des in Abschnitt 3.6 vorgestellten Präprozessor-Verfahrens zum Dixon-Schneider-Algorithmus.

<sup>6</sup>Zeitmessung auf einem PC mit 650 MHz Pentium-III-Prozessor und 1 GB Arbeitsspeicher

<sup>7</sup>Zeitmessung auf einem PC mit 700 MHz Pentium-III-Prozessor und 384 MB Arbeitsspeicher

<sup>8</sup>Zeitmessung auf einem PC mit 450 MHz Pentium-III-Prozessor und 512 MB Arbeitsspeicher

Hierzu eignet sich GAP [39] am besten, weil es einen sehr flexiblen Umgang mit „unvollständigen Charaktertafeln“ ermöglicht. Innerhalb weniger Sekunden fördert das System auch die restlichen 20 Elemente von  $\text{Irr}_{\mathbb{C}}(G)$  zu Tage und produziert so die in Anhang C abgedruckte konkrete Charaktertafel.

Aus dieser Tafel liest man ab, dass die Gruppe  $G$  einfach ist und dass  $H = \mathbf{C}_G(z)$  für die 2-zentrale Involution  $z \in S \leq H \leq G$  gilt. Satz 5.1.1 liefert deshalb die Behauptung.  $\square$

## Anhang A

# Die Rudvalis-Gruppe als Untergruppe von $\mathrm{SL}_{133}(5)$

Auf den folgenden vier Seiten sind der Reihe nach die Matrizen  $\mathfrak{M}(k)$ ,  $\mathfrak{M}(f)$ ,  $\mathfrak{N}(t_0)$  sowie die Transformationsmatrix  $T$  aus Unterabschnitt 5.4.3 explizit abgedruckt. Es gilt

$$\mathrm{Ru} \cong \langle \mathfrak{M}(k), \mathfrak{M}(f), \mathfrak{N}(t_0)^T \rangle \leq \mathrm{SL}_{133}(5) .$$

Selbstverständlich existiert jede einzelne dieser Matrizen auch als Datei im ASCII-Format. Alternativ zu  $4 \cdot 133^2$  Ziffern tippe man bei Bedarf eine kurze E-Mail an den Autor:

`kratzer@exp-math.uni-essen.de`

```

44.
1.
24.
414441.
4.2322.
2.3322.
33.2.4.
34.4.
3.1.1.
244.14.4.22122.13.312.23322412.141.2234114.42.13.4.1.24.
23.31413431141.2442.34242132344123.3122.2.341.4.43.2.2.
21344324223.13433242142113.2233.32213224444414.2213311.3.
4134433.432321121433123213.343.1114422444.1433132444.4111.
3412334.3.3114231.4.3.33434.421.4332.43314233244.3143322.
344.13.34.2.4114334113.4423.444.43114344113113311134.4433.2.
22222.443324343143131.332.31.33.1.3.4.323.1.34.2.41222.
1431.34.3.34.2.13312433.2111131212113.2.3224.4.311.2243.
22.231.314414111242333.3.32.3.34.34.33115212.4.1.2233.
334.1.3131133141.22334.2.11223214.222.241142143332.222214.
2144.3431.3.43.3.44423.1333.14241.11.3.1242123.111344324414.
324.32441224.114.333.34422312312224.4.4343.11.131241.12.
324.412.13321214.123.44.3243241.4.214.143.321232.44.12.4.
4144.414412.4443.31431324123.3.113.32.24443.133.1.4.131231.
14423.212.21314123.23223.2312441113423.431.24.21.34314113.
134.214.41.13.2333334432211143441.22243.14242344.1.23323.
4111142324.1.4.4.333.34.2134.3321.2431.4444.3414412.
4311.1121213341332212.133.2243324133.2323124.3333.14.24.1.
243.4.1.142441.3.12314121444.3214143441224142211.2241132.1.
2323.4.4341122.31.124224.33123242.313.123.12.1.31.1314.4.
21213431.3.1214.244.21424.113.4431.2.442.4413.34441342.
4111142324.1.4.4.333.34.2134.3321.2431.4444.3414412.
4.44.1214.2134441.3.3412341.2413.444313.24222.2333.244224.31.
2122.334.4134321.111.1433232431112424243.421223.4311.442.3.
33.2334143423.122.422.24124.33.1123.413232.11.4443.1431212.3.
3331.213.121331.21441221.41321.214.3.434.3124.44.3121.321.
2.1142.44.23233.33212244334.4424.121.243.133323341.321.43.
443.1.112444112.31.22.22.1.3231122.334143141.12.434.3144.
241222.4214422241.13314123.4324.22144214323.2.34443.2.22.
333124.311.214141.213.44124.242.331434214111233123.243.
4.4143323242.31.2111.311.413.2.2443312324.212.431313.2.
134112243141.3.34.3433232.421243143.12.4.22111344.141.2244.
32.31121.14122.24.412.41111.3.34443222344.12.1.311341.4.2.
244211141.132.4212133134423244.12243.42.124433313141424434.
442.213.121331.21441221.41321.214.3.434.3124.44.3121.321.
12312.2442.43344112.3.4.11.143323132121343.4443.341111441.
4.41233.4.1214344.42231423334.31.3411424.21434414.4.22.2.
341311.4.24.2133.423331.32.4131.2231.3442.413.113.1121.31.
2242411.121.442.43.324243132143233.4.12112312121132424133.
44332.13232314212312.12433.43124.1.42241.21.43.21.334234.
33.3.3141.11.221.221311311.2.1.31.12441443112.12.13.31114.
141424312243323431.414.424322.1.4132.32334324.231234334.32.
21.2112122.33144244.212331112.4.31114223.314.24244112244.2.
33.3442.21.2143434.113.114233.1.2143434.321.43.21.111.3.
44224.31.23443.3324.2112.312.243.231344311214224.41.
21.24.123312.11421111231.343442.322.11144314.14.13.221212.
11.3.2234.21422444.11422343111442133442342.211333.1233243141.
3.312122.144443.231.24241423.41442334.4.222413241.4.31.
43212142443.3114.31132.43.1.4111.3.432233322124.31.1.33.
1422123311344114.3424413431233432.413423312.234.4411122412.
4.4224413.1.4412.32.34.424114.1.3231411.44.2.3224.13.33313.
224.2.44124444331.32.2312212.1321111.13224.442.2.224.223123.
33212.134313212.121333.4323.32221.121333.320221.
144.4.13134.3.2332144344421133.4332.3.332.122241.41331.
1.4.12.14.2114.2423.3424.2.2.2.34241.2.132233.33412132.
332433.2432431.23.4323134241112442214433.1143.143421213.22.
43213.1.4444234.4431.43.1.1.123.14.2242.344234.241144423.23.
3.131334.321.32.3423.32333.244341.441233.2434.2134.
233.43121421.4214.43222131434.124.143431243322413122.4344.
43112141.2.3314.4.342143.11413.14433.3.232142431211414133.
4.4323.34.13.113212243.33.234441342112.3213.342.34.33.131.
1422.231533.4.2.34.4412.141.41.43334111.1333241213.2222.4.1.
43134.43331411.32334441.442341122.4.213432224.3143.41.434.22.
43134.443.344.4.44231.2.231312214.4.34441142131233234.2.14.432.
3441.4223144423444.424314.4411312211222132.14.14.2213.442234321.
212334.234.313.3343.22144432434211221.2113233.41442.33222222.
242233.234.313.3343.22144432434211221.2113233.41442.33222222.
14232313.333.21211.4412432.2.13114.34.423.14234341.12323112124.
4334122134434231.34321.2232.343.431.34334111.1333241213.2222.
4.3.33413.12312.32311.14.14.44.31.41.223.33.231232.122413.
242233.234.313.3343.221431.143434.321.43.21.413412.314.
21414.42423.1.21.432.44333.3.243.244142324312231.4.1323.22.4.3.
11211311.134.21222.1.144.2.112.2321.432.3.24.222141234421112.
3143113323.144234.341.223432233412143331.21214332213432434.13211.
4333344.4.22122332.4.31.1342.221.323332434.2.1.1.2.2.12.4.
3234224.4334.1.2312.1133.3321122441.34334.3.4.3412.22.
4.2.12344.3123433.13142331111131244141.441244114.134142134.41.
11.223.242.1.142413134241.4.2.3.141.32223.432244332124.4.
1244.1.122.2.4.1.142.41.411.22.3.21.22113114211221.12.
4331.13.14143.334414.224111434421.244.21.43214211421.13.
24211121113242322333412.4.2.3443.433424432.1412412224322.134.212.
223243.13.244.14.41242312.3342143.224.121321433344.1334.421212.
43343121.123423.421.23.2423334.2.122411312.122113411.24.
33.332131.3.1423144.13144.43224441.1.4.3124222.24.
34.123212324324.4241322433.44.232311121.33.3.4.42.34141314331.
4444442.31.23144121144142221124221214.42341213.2224.331.33.2132.
33213.234.4111.14313122.42243.4333.414121.21411.31.212.1.43.
1243224221344331313.4121.1.143414.14443.34414.33312422132131.
22.13.12122.311322.312.1.4314.41.13222.31234124.3.2.3.412.
323412444232.21133431.212.43.324.14333212414.42233.11.133311.13.
241.4.211.3342331334.2213331.31112.411143.2.3443.11.31413431.
442.3341412433114443.34411.3.4.1.21.2.311.13.241.43133.44.1.
1.43.44332.3441.31342342.31414.41.334.44.52.312.3323331.4242.
34.24121412.13331.4111443.31231.131.41111.41432212.1432124.3.
121121.311233244.14.23.31.14.31.44.131414221322.421.3.2312.31.
23312.421234232212141213423421.21.443211.132.4112.43.42441.31.
342414124.244.23113412.41341144.142.1.24141241122.42331111441.
3.131334.321.32.3423.32333.244341.441233.2434.2134.
214214.12111222214331141344.2.1.2133.4232.33.311313.21.123244.1.
431342143141343.3.332.4.341242.1.112421143.3.111312314.4111.
1.2111443112111432412111.13.414243.13133324111.421.4.2421222.
4344.44113243.13.434311.122341431.132.4112.131.1.143.144142.24.
43.1121.442.21.113.33.1321441242.3.13423113141.1.112424244.
3.221441.1.1144142134213142.4441242244.111.2.42324.13334.11.2.
4233443.323.332.41.313.1.12.123121122.31.422412141341112243.
1411.41143.42.212.42414.14.4443433.4414.3221.1.43.13344.31.4.
3313.3214.3.4412.22.143224.4444.2412413.23.124.41.41.22411.4.
141134232244.2.3.44.41223.3.14223144423423324.3312224.22.224.21.
3.22212131.1.33234.14213322324412412312442333332132244.3344.3.33.
42322.211.2.14223.321243.4.3433442.343113313.23424211222139.2.
44313142.2.3312123422.12411342433144331331.2.114.312211441.243.
2314341.31212313.32.33.1334342.14241.244124224.13.12.444.
223411341.22.2411411.233423.2.3322131222.21.12.312431.2112.2.
42322.42.14.4434.422.3313143323313321.443.1.114.21112.3431311142.
13134.131242344121144212.4224114.4422.4.1442224.233.2422.42.42.
41433334132.21.4.213114313.34.4222321.44.1.2.2.131413.43414.
1.232121244.33444212332322313.134.41432311.423143341.134.34143.
3.43332.42.1421224431133422112432.123.332.24111311223121.34.334.
32.424214444323221.21223.414.131.21.243.331.32.29.231.2424.
44314131.12.4242.22.44.421.442.332.431.34414.22331343343222.
3.4213132434422.2.243.42.4113.14312443.4.4.13323.4.124434.
3.1323.33.14.212332.1211.32431324423331414.4214234.334.41224.41.
1.3.1423123.32422421324.44.22.1424.2244222.33.23343231.324.
43.1411444.42341.3.22.3.44.41.23414434141.4.1.3434.232.

```

```

412
43
12
4 2144
13 44
12 44
4 2 2
4 2 35
32114224124141 444223 34241334 243 324121 3222 142 1411114
4 1 34 123 232 4 1433 313211 2123123342224414222 4 2 432314
13432243 32 3143213212 3 4124 35324114242 1 2322142222
3 424344222442 3331 1 324124 4 22 3 4 244222444 312 214
33 223114322344 243314424 422111 4 13 14121124 34 21122132
2222324 2 3433134 4 3331324 44 3333 3343 4224 2 2 342 4
412 3313 3434441 442 243 31232 3 3 114421 211 34 3142 34
12 214 1343 314 21344111 43 1244141124111331121 433 334 2123
3 42433333 24 3 123 3 43 1443244 23112223 422 224 431441
144223122 4 213 114343 4 314 34 12 13242 23321 12 12 2 2
1414 244 3112314122224 31 432213213443312 21 3 4 1334422 2
21143142 21111244 433 4411 31441422 112 3 3 234 32142 43
1214321 132441 24 41 231423 32341241 113 231441 4234 33 31
34233 2 32 3344 211133 12211 3412 14224 313 24 123 41444 2
422342 42 332 12321342412 44143 4412 4 4 431 14441234443 22
44222441 4 4234121 1412 31443 4314332 1 234 3314444444 4
412 21 14324 1242 211442 331 3 43 333234 323113 3
11221 433421112243 12112121 2142413422321 2 124132113233243
12434 344 433 214413323 442 3241313 212 333 43412214332 11
231 33321443231223 3224434 1344143 14133 1422332 1 31 44 123
2341234 33 321 34142114 4 244312221322243 31213 3111341314
1 433341 22 3 2 312 11233421 2 4222 443 1213122 1 33
2144244321 14144 3231 1 4432332441331 1323334 1222 21431 214
2414124344 2223232111421133433311 231 23324 244442132212 44
222 3 44422241142311 34 4113 224 3322 3 313432 3 2342444
333 44223214343 44 12 4432 34 42 12434 331424124 241 4214
4 42332322343434 3131233 1144 3 33 4241343222333 4 43 214
211 211142 4231 131 13234242413314 42333211 22133 41 2
42 42433 21 12 42 132122121 1 213413 13112341 4 3 2 1 22422
11331 3 44 24114 3 1 11412434221442432341422231 2 43332
4 2134134323 4 41 141 42 43 3413 221334 23311 2 14 41214
422 144 421 33 421 44 1133 2 2 4 311 434 4 41 13143134
41131132421 12 334424312 112441 2 13 122 1342234 21234 333 2
2 1124 333 4 432421221244 213 2 1 44122424122433 31431 4
432134 1444413 21211214121 31412 223114221133243114144 3
321134 3 44 3413 214343 444 22 314 12334 4411 4 431
211 11244 2133431 2 2341143322444 1444242 1121144142 4
3241331 13332 44321343 232311 3323 43213 22324314244214 1
234232 21 2424 2 141131 3424 32133 24113422 232122 31134
3 121143343 2121 2 24 412 43 3413 221334 23311 2 14 41214
12 3 243 4 141221213 31122411241332341 214 323 4 121421
14134 1 42 3133311 311 4 24221224 3 1 1 4 222 43443 3211 1
11132433 343333 312 1334414413 4423111414341 41 114 4 131
2 12 3 34 132411 22223 31124312 2 22223 31124312 2 24 2
4 212114412 32141134222 234 23343 422 1212 241433 3 3 43
342134222312 11222443344422 112311242432 13224 3 1 121 1
441 222 33243 3311222 3 2 1322 143 3132 342134 32231442
14 42113421324 13343233112214 21422433 4244431 34
242 24 32413141221221 313431112433 3 3 243 131 3214
34111243 12 24 21 234 422 131 242223413 4 44131 122244221 4
22144 1 12424112211 421132 1 31143 24 22212314113223342 22
34 14 22 23132313 131 324131 23132 411 334 431 3 4322 13
24 1434 1 424 11344 11344 121332224244 1 433 332 322 13
12 4 32311 14222 334334 221414411 433 34213 3123112231212 3
131244121 4424341444322433413 12 33 1 114 1 3 4 43432124
2324311 333 344 4131 433342241424443 1443 2 13 2443 32 43
44213 4 4421 214331 13323 31 4412423 42 31213333134 343221
1314421222124 2 323131 42423 4 3 23432242311443223 3
42213 12233313 1 223123 3414443 2 4 2413 434343112214423
4 44234223 43114 323 321 244 321 13 143322 423 3 3 3334
43 2 4 4 34144431 131 422 13 3432 1 314 121333143 3323 143 33
2432214 332 24421131212 321341432 22314321 321341414 31
114111 11 14431223 234411312 332132224 43314 43421414 242 31 3
111 32 24444244 42 111 111444443 13112212434334 321 22 1 4243
312242313 114 1234 3 4 13 1142 3112242 42131 122 4 431441
321 14323 224 3412311 1133441 212123 323121 143133 121 34332334
3344 2 14343 12 14 214 23 1433 22 31 123 123 21 1321 14122
2 333324 431211 32 3 31 21 4 42 3 42 4 42 431414233 4 2332334
2243231 31 1333 1221123 422211 12332 244114411 1211 1123 3124
2324311 23 14 32313 43 4324 21224 2323422 12344 4223 324 24111
344 2 14343 331 221 14 4142 14343 433 3214 32 3413 123434244
343334331244224343 414223233212 1 42 1432411 3311 123331 11333
2232 13421143314311112 32311 43 4 433 32 143233243 23 434223 44
1 13334 34 23342 44 141332321422244313 2 4 2234141 2 124 24324
312212142313 3 3343431 31 4 14 3 41 222144411331413 123321
2 24234122313 31 12 2 143111214 34 4 44432413322 112441244
1 212221 2411243 32243331113233332 424 331344 3 2421341 41 1111
2 11 34441432412132414241 24131 132 14 43 33 4 43 22131214444
4334 4 2342 344431 24343 33434124 423 4 3111431442 31 23434
4344 2 1434331 221 14 4142 33442123 43112 32221 3 34 32
4 344234124233 124442122 243 24244 222123 1 12 32124112 4
1 2 314442 4 144 22 334 234132444 34123 13213 3442 3 1214 121
412444432 4 2 14 342 24 322 332114341314 311322 3324233 3124112
3312212142313 3 3343431 31 4 14 3 41 222144411331413 123321
2121432413412211231211222 4 1 4 4 2 141 214134143 12 423 21
224 4341232413443 3123 1132122 1143121 12444124 323 4144 13423
4 22124113312 131 322 233 221 4 43 1 3433 44 1 122 3314 213 12
4231 4244 32 41 3 43211 32214 34112141132123412423 2434241342
3144 3 2212 1111242 241322 4 14421414 4343 3 414 4221143334441
322 4232124 43 4234421 22 3 2 21 2 23 1 4444142332 23 24
4412 3 33 1 411421 32243 1 2 12414 4324243413 21112433413 1
4214322333443313244 4 33441 241443324 4 1233213 2 3341421 443
34322 43 3324344 3 3213 1 3 2344323223 44433234244 41414
4 1344123424213412421314 1 23312 1 24 1 4 323 21 1212 41 2322
44 4324424 3332 24 22 141441333224123 2111134341 3444 23323411
12 434314 2 11134 42342 411322 13 41 4 14431 113 4 3 412124
3442 43123443223 242 4433 313311211 44 1 13 433424 423 3 33
1 1 333311 4 2 323344 22411141322343444 4 1 3234 44 4112 4233
2414 144 4 444 4224341 33221 14 4131322 22 111433 33 22212 4
4943214333 31 3 13234 14 4 4 2 313 133 1 4321 11343 324 1112
4334412 232131 1243311 21332413312 2 3 1342413 2213 1 32 2233
12 2421 212 2 2133222131 222211132 21 12 122341131242144433 4
12 3 23124141442343341444 3232 14131214423143341412434 1323 3
12 3 33434 4 3122 4332 2213114 1221412 41 2 4323 333 44 334
322 1 233214223431142 4141113 2 3 14 113312 124 3 141 42 1244
33343412122 4443 144423344432344144124441413214 414 11142 2444
12321411321311242331123432 3 4114131 3321 242 1213 3
1 114 324241 2421 1442122121 314 1 144 24 2 13 4 4231413
1441112 242 14113 13 3234 43221 44 2 14111423 32 34 123 14 13
321242212 3 3 3 112212131 21 2244223 324413212 4 1 12 32 3222
12314131 41124 1 41213442 44 321323 44113131 3213 4322324 22
14143214 4 44434 32141 21132121213 341 211 34 3222 43242
13 214 23133 22143 4343132 134423 33 424 3 1432 3 4342242 314
1 11413241 24343 2 1214232 4 313434241 21 23134334243241 4423
13143421244324 312 2442 34132 1 12133 43241111 3212 4 22223244
312114214 31342 1 44 13224341213 21 1222243 2441423 21411313131

```

[illegible]



[illegible]



## Anhang B

# Relationen aus dem Doppelnebenklassentricks

Genau wie die Matrizen in Anhang A können auch die Permutationen  $k, f, t_0$ , welche eine zur Rudvalis-Gruppe isomorphe Untergruppe der symmetrischen Gruppe  $S_{593775}$  erzeugen, per E-Mail vom Autor angefordert werden. Auf Empfängerseite sollte jedoch mindestens 13,5 MB Plattenplatz frei verfügbar sein.

### B.1 Doppelnebenklassenzerlegung

Unter Verwendung der Bezeichnungen aus dem Beweis von Lemma 5.5.1 beschreibt die nachfolgende Tabelle ein explizites Repräsentantensystem  $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_{22}\}$  der  $H$ -Orbits auf der Menge  $\Omega = \{1, 2, \dots, 593775\}$  sowie Elemente  $r_i \in \pi_G(G)$  mit  $1^{r_i} = \gamma_i$ ,  $i = 1, 2, \dots, 22$ :

Punkt $\gamma$	$ (\gamma)^H $	Konjugator von 1 auf $\gamma$	Punkt $\gamma$	$ (\gamma)^H $	Konjugator von 1 auf $\gamma$
$\gamma_1 := 1$	1	$r_1 := \text{Id}_\Omega$	$\gamma_{12} := 914$	10240	$r_{12} := t_0 f t_0 f^2 k t_0 f t_0$
$\gamma_2 := 2$	30	$r_2 := t_0$	$\gamma_{13} := 307$	12288	$r_{13} := t_0 f k t_0 (f t_0)^2$
$\gamma_3 := 16$	240	$r_3 := t_0 f^2 t_0$	$\gamma_{14} := 819$	15360	$r_{14} := t_0 f^2 t_0 f t_0 f^2 t_0$
$\gamma_4 := 8$	480	$r_4 := t_0 f t_0$	$\gamma_{15} := 422$	30720	$r_{15} := t_0 f t_0 f^2 t_0 f t_0$
$\gamma_5 := 160$	640	$r_5 := t_0 (f^2 t_0)^2$	$\gamma_{16} := 190$	61440	$r_{16} := t_0 (f t_0)^3$
$\gamma_6 := 76$	3840	$r_6 := t_0 f^2 t_0 f t_0$	$\gamma_{17} := 365$	61440	$r_{17} := t_0 f^2 t_0 (f t_0)^2$
$\gamma_7 := 85$	3840	$r_7 := t_0 f t_0 f^2 t_0$	$\gamma_{18} := 433$	61440	$r_{18} := t_0 (f t_0)^2 f^2 t_0$
$\gamma_8 := 17336$	4096	$r_8 := t_0 f k (f t_0)^5$	$\gamma_{19} := 986$	61440	$r_{19} := t_0 (f t_0)^4$
$\gamma_9 := 1206$	5120	$r_9 := t_0^2 f^2 t_0 f t_0 f^2 t_0$	$\gamma_{20} := 1325$	61440	$r_{20} := t_0^2 (f t_0)^4$
$\gamma_{10} := 39$	7680	$r_{10} := t_0 (f t_0)^2$	$\gamma_{21} := 3047$	61440	$r_{21} := t_0^2 (f t_0)^2 f^2 t_0 f t_0$
$\gamma_{11} := 808$	7680	$r_{11} := t_0 (f^2 t_0)^2 f t_0$	$\gamma_{22} := 1871$	122880	$r_{22} := t_0 f^2 t_0 (f t_0)^3$

Um möglichst kurze Relatoren zu erhalten, wurde mit Hilfe von MAGMA eine Basis

$$\{\beta_1 := 27, \beta_2 := 4, \beta_3 := 8, \beta_4 := 18, \beta_5 := 39\}$$

samt rekursiv definiertem starken Erzeugersystem  $s_1, s_2, \dots, s_9$  von  $H$  berechnet. Ordnung und Stabilisatorenlevel dieser Generatoren sind der nächsten Tabelle zu entnehmen:

Erzeuger	Ordnung	stabilisierte Basispunkte
$s_1 := k$	4	$\beta_1$
$s_2 := f$	5	—
$s_3 := kfk(f^2k^2)^2(fk^2)^2f^2k^3f$	4	$\beta_1$
$s_4 := kfk^2fk^2f^3k$	4	$\beta_1, \beta_2$
$s_5 := kfk(f^2k^2)^2fk^3f^4k$	4	$\beta_1, \beta_2$
$s_6 := k^2s_5fs_5s_4f^4k^2s_5s_4^{-1}$	2	$\beta_1, \beta_2, \beta_3$
$s_7 := ks_5^{-1}s_4s_3s_4s_3ks_5s_3^{-1}2s_5^{-1}s_4^{-1}$	2	$\beta_1, \beta_2, \beta_3$
$s_8 := s_4s_5fs_4s_7^{-1}k^3s_5^{-1}s_7^{-1}k^3f^4s_5^{-1}$	4	$\beta_1, \beta_2, \beta_3, \beta_4$
$s_9 := s_8^2s_4s_8^2s_4fs_3s_6s_5s_7s_4kf s_4s_3^{-1}f^4k^3f^4s_3k^3$	4	$\beta_1, \beta_2$

## B.2 Relationen der 1. Kategorie

Für die 22 Zweipunkt-Stabilisatoren

$$S_i := \text{Stab}_H(\gamma_i) = \langle y_{i,1}, y_{i,2}, \dots, y_{i,\ell_i} \rangle$$

sind die hier angegebenen Erzeugersysteme minimal — im Falle  $\ell_i \geq 2$  ist  $S_i$  nicht zyklisch, im Falle  $\ell_i \geq 3$  gilt  $S_i/S'_i \cong 2^{\ell_i}$ .

Erzeuger	Ordnung	Erzeuger	Ordnung
$y_{1,1} := k$	4	$:$	$:$
$y_{1,2} := f$	5	$y_{6,3} := s_8^{-1}s_6s_4s_5s_3ks_3^{-1}f^2k^3$	2
$y_{2,1} := s_6s_7s_9s_4k$	4	$y_{6,4} := s_7s_5s_9k^2$	2
$y_{2,2} := s_9s_4s_5$	4	$y_{7,1} := s_8^{-1}s_6s_7s_5s_8s_9$	2
$y_{2,3} := s_8^{-1}s_7s_4ks_3fs_3$	8	$y_{7,2} := s_8^{-1}s_9s_8kf s_4f^4$	4
$y_{2,4} := s_4$	4	$y_{7,3} := s_8^{-1}s_6s_9s_4k$	2
$y_{3,1} := s_8^2s_6s_9s_5$	2	$y_{7,4} := s_6s_5s_8ks_3^{-1}f^2k^3f$	4
$y_{3,2} := s_8^{-1}s_6s_7s_4^{-1}s_5^{-1}k^3$	2	$y_{8,1} := s_6s_9s_8s_4^{-1}s_3ks_3^{-1}f^4k^3f^4$	3
$y_{3,3} := s_8^{-1}s_6s_7s_9s_5s_3^2f^2k^3$	4	$y_{8,2} := s_6s_7s_4s_5s_9fk s_3^{-1}$	5
$y_{3,4} := s_6s_4^{-1}s_8s_3^{-1}f^2k^3f$	4	$y_{9,1} := s_8^{-1}s_4^{-1}s_8ks_3f^2k^3f$	6
$y_{4,1} := s_4s_9k^3$	4	$y_{9,2} := s_8^2s_6s_5s_8s_3^2s_4$	2
$y_{4,2} := s_8^2s_5kf s_4f^4$	4	$y_{10,1} := s_6s_5s_9s_8k^3s_3fs_3$	4
$y_{4,3} := s_8s_4^2s_3s_5fk s_3^{-1}$	4	$y_{10,2} := s_8s_4s_9s_5s_3ks_3^{-1}f^2$	4
$y_{4,4} := s_8$	4	$y_{11,1} := s_8^2s_6s_5s_9$	2
$y_{5,1} := s_8s_6s_4s_5^{-1}k$	2	$y_{11,2} := s_8^2s_6s_7s_5s_4^{-1}k$	2
$y_{5,2} := s_8^{-1}s_9s_4s_3ks_3^{-1}f^4k$	4	$y_{11,3} := s_8^2s_7s_5^{-1}s_3kf^2k^3f$	2
$y_{5,3} := s_6$	2	$y_{11,4} := s_6s_5s_9k^2$	2
$y_{6,1} := s_7s_5s_4^{-1}k$	2	$y_{12,1} := s_4s_5^{-1}k^3s_3f^4k$	4
$y_{6,2} := s_8s_6s_7s_4^{-1}ks_3^2f^2$	4	$y_{12,2} := s_8^2s_5s_8s_3f^4$	4
$:$	$:$		

Erzeuger	Ordnung
$y_{13,1} := s_8^2 s_6 s_7 s_3 k f^4 k$	4
$y_{13,2} := s_8^2 s_6 s_7 s_4 s_5 s_3^{-1} s_4 f^2 k^3 f$	2
$y_{14,1} := s_8^{-1} s_6 s_7 s_5 s_8 s_9$	2
$y_{14,2} := s_4 s_5 s_3^{-1} s_4 f^2 k^3 f$	2
$y_{14,3} := s_6 s_7 s_4 s_8 s_9 k^3$	2
$y_{15,1} := s_8^2 s_6 s_7 s_4 s_9 k^3$	2
$y_{15,2} := s_7 s_5 s_8 s_9 s_3^2 f^2 k^3$	4
$y_{16,1} := s_8 s_7 s_4 s_3^2 s_4 f^2 k^3$	4
$y_{17,1} := s_8^2 s_6 s_7 s_5 s_9 k^2$	2
$y_{17,2} := s_8^2 s_6 s_7 s_4 s_5 s_3^{-1} s_4 f^2 k^3 f$	2

Erzeuger	Ordnung
$y_{18,1} := s_6 s_7 s_5 s_9 k^2$	2
$y_{18,2} := s_8^2 s_6 s_5 s_8 s_3 k f^2 k^3 f$	2
$y_{19,1} := s_9 s_8 s_3 k s_3^{-1} f^4 k^3$	2
$y_{19,2} := s_8^2 s_6 s_7 s_4 s_8 s_9 s_3^2 f s_4$	2
$y_{20,1} := s_8^{-1} s_6 s_7 s_5 s_9 s_4 k^3 s_3$	2
$y_{20,2} := s_4 s_9 k s_3 f k f^4$	2
$y_{21,1} := s_8^2 s_4^2 s_9 s_3 k s_3^{-1} f^4 k^3$	2
$y_{21,2} := s_8 s_7 s_5^{-1} s_8 k^3 f k f$	2
$y_{22,1} := s_6 s_7 s_5 s_9 s_4 s_3^2 s_4 f k f$	2

Außer  $y_{1,1}^{r_1^{-1}} = k^{r_1^{-1}} = k^{\text{Id}_\Omega} = k$  und  $y_{1,2}^{r_1^{-1}} = f^{r_1^{-1}} = f^{\text{Id}_\Omega} = f$  gelten mit den bisher definierten Bezeichnungen folgende 54 Relationen in  $\pi_G(G)$ :

$$\begin{aligned}
r_2 y_{2,1} r_2^{-1} &= s_8 s_6 s_7 s_9 s_8 s_3 s_5 f k f s_3, & r_7 y_{7,3} r_7^{-1} &= s_8 s_7 s_4 s_5 k^3, \\
r_2 y_{2,2} r_2^{-1} &= s_8 s_6 s_9 s_8 s_4^{-1} s_3 s_5 f s_3, & r_7 y_{7,4} r_7^{-1} &= s_6 s_9 s_8 s_4^{-1} k, \\
r_2 y_{2,3} r_2^{-1} &= s_6 s_7 s_5 s_9 s_3^2 f^2 k^3, & r_8 y_{8,1} r_8^{-1} &= s_8^2 s_5 s_8 s_9 s_3 k f k f s_3, \\
r_2 y_{2,4} r_2^{-1} &= s_8^{-1} s_7 s_4 s_5 s_9 s_3^2 f^2 k^3, & r_8 y_{8,2} r_8^{-1} &= s_8^2 s_6 s_9 s_4 s_5 s_3^2 s_4 f k^3 s_3, \\
r_3 y_{3,1} r_3^{-1} &= s_8^{-1} s_6 s_7 s_4 s_8 s_9 k^3, & r_9 y_{9,1} r_9^{-1} &= s_8 s_6 s_5^{-1} s_8 k^3 s_3 f^2 s_3, \\
r_3 y_{3,2} r_3^{-1} &= s_7 s_4 s_9 k^3, & r_9 y_{9,2} r_9^{-1} &= s_8^2 s_4^{-1} f k^3 f^4, \\
r_3 y_{3,3} r_3^{-1} &= s_8^{-1} s_4^2 s_9 s_8 s_3^2 s_4 f^2, & r_{10} y_{10,1} r_{10}^{-1} &= s_8^2 s_7 s_4 s_5 s_9 k^3 s_3 f s_3, \\
r_3 y_{3,4} r_3^{-1} &= s_6 s_7 s_5 s_9, & r_{10} y_{10,2} r_{10}^{-1} &= s_7 s_5 s_9 s_4 s_3^{-1} f^2 k^3 f, \\
r_4 y_{4,1} r_4^{-1} &= s_9 s_8 s_4^{-1} k, & r_{11} y_{11,1} r_{11}^{-1} &= s_8^{-1} s_6 s_4 s_8 s_4^{-1} s_3^2, \\
r_4 y_{4,2} r_4^{-1} &= s_8^2 s_7 s_4 s_8 s_9 s_3 s_5 f s_3, & r_{11} y_{11,2} r_{11}^{-1} &= s_6 s_7 s_4 s_5^{-1} k, \\
r_4 y_{4,3} r_4^{-1} &= s_8 s_4 s_5 s_9 s_3^{-1} f^2 k^3 f, & r_{11} y_{11,3} r_{11}^{-1} &= s_8^2 s_7 s_4 s_9 k^3, \\
r_4 y_{4,4} r_4^{-1} &= s_8^2 s_4^2 k s_3^2 f^2, & r_{11} y_{11,4} r_{11}^{-1} &= s_6 s_7 s_5 s_4^{-1} k, \\
r_5 y_{5,1} r_5^{-1} &= s_8 s_5^2 k^3 s_3 f k f s_3, & r_{12} y_{12,1} r_{12}^{-1} &= s_8^{-1} s_6 s_5 s_4^{-1} k f k s_3, \\
r_5 y_{5,2} r_5^{-1} &= s_5 s_9 s_3^2, & r_{12} y_{12,2} r_{12}^{-1} &= s_8 s_4 s_8 s_4^{-1} s_3^2 f s_3 f, \\
r_5 y_{5,3} r_5^{-1} &= s_8^2 s_7 s_4 s_9 k, & r_{13} y_{13,1} r_{13}^{-1} &= s_8^{-1} s_6 s_4 s_8 s_9 k s_3^2 f k^3 f^4 k, \\
r_6 y_{6,1} r_6^{-1} &= s_8^{-1} s_9 k s_3^{-1} f^2 k^3 f, & r_{13} y_{13,2} r_{13}^{-1} &= s_8^2 s_5 s_8 s_9 k s_3 f k f s_3, \\
r_6 y_{6,2} r_6^{-1} &= s_8^2 s_7 s_5^{-1} s_8 k s_3^{-1} f^2 k^3 f, & r_{14} y_{14,1} r_{14}^{-1} &= s_8^{-1} s_9 k s_3^{-1} f^2 k^3 f, \\
r_6 y_{6,3} r_6^{-1} &= s_8^2 s_7 s_5 s_4^{-1} k, & r_{14} y_{14,2} r_{14}^{-1} &= s_7 s_4 s_5^{-1} k^3, \\
r_6 y_{6,4} r_6^{-1} &= s_8^2 s_6 s_7 s_5 s_8 s_9 k s_3 f k f s_3, & r_{14} y_{14,3} r_{14}^{-1} &= s_8^2 s_9 s_8 s_4^{-1} s_3 f k f s_3, \\
r_7 y_{7,1} r_7^{-1} &= s_8 s_5 s_3 s_5 f k f s_3, & r_{15} y_{15,1} r_{15}^{-1} &= s_8 s_6 s_4 s_5^{-1} s_3^2 f^2, \\
r_7 y_{7,2} r_7^{-1} &= s_8 s_7 s_4^2 s_9 s_3^2 s_4 f^2, & r_{15} y_{15,2} r_{15}^{-1} &= s_6 s_7 s_5 s_9 s_3 f k s_3^{-1},
\end{aligned}$$

$$\begin{aligned}
r_{16}y_{16,1}r_{16}^{-1} &= s_7s_5s_9s_3fks_3^{-1}, & r_{19}y_{19,2}r_{19}^{-1} &= s_6s_7s_5s_9s_4s_3fs_3f, \\
r_{17}y_{17,1}r_{17}^{-1} &= s_8^2s_6s_7s_4s_9k, & r_{20}y_{20,1}r_{20}^{-1} &= s_4fkf^4, \\
r_{17}y_{17,2}r_{17}^{-1} &= s_8^{-1}s_5s_9s_8k^2, & r_{20}y_{20,2}r_{20}^{-1} &= s_6s_5s_4^{-1}s_3^2f^4kf^4, \\
r_{18}y_{18,1}r_{18}^{-1} &= s_8^2s_6s_5s_8s_9ks_3fkfs_3, & r_{21}y_{21,1}r_{21}^{-1} &= s_4s_8s_9ks_3^{-1}fks_3, \\
r_{18}y_{18,2}r_{18}^{-1} &= s_8s_6s_5s_9s_8k^2, & r_{21}y_{21,2}r_{21}^{-1} &= s_8^{-1}s_6s_7s_4s_9s_5s_3kfkfs_3^{-1}, \\
r_{19}y_{19,1}r_{19}^{-1} &= s_8s_7s_4s_5s_9s_3kfkfs_3^{-1}, & r_{22}y_{22,2}r_{22}^{-1} &= s_8^{-1}s_5^{-1}k^3s_3fk^3f^4.
\end{aligned}$$

### B.3 Relationen der 2. Kategorie

Der zweite Schritt des Doppelnebenklassentricks im Beweis von Lemma 5.5.1 führt als Erstes auf die evidente Beziehung  $r_1t_0(r_2)^{-1} = 1_H$ , darüber hinaus aber auch auf 171 nicht-triviale Relationen in  $\pi_G(G)$ :

$$\begin{aligned}
r_2t_0(r_2k)^{-1} &= s_8s_6s_7s_4s_8s_9k^2, \\
r_2kt_0(r_1)^{-1} &= s_8s_6s_7s_4s_8s_9k^2, \\
r_2ft_0(r_4)^{-1} &= 1_H, \\
r_2f^2t_0(r_3)^{-1} &= 1_H, \\
r_4t_0(r_4s_8s_6s_4s_8s_4^{-1}k)^{-1} &= s_8^2s_6s_7s_9s_4s_5k^3s_3fs_3, \\
r_3t_0(r_3k)^{-1} &= s_8^2s_6s_5s_3fs_3, \\
r_4kt_0(r_2kf)^{-1} &= k^2, \\
r_4ft_0(r_{10})^{-1} &= 1_H, \\
r_3kt_0(r_2f^2)^{-1} &= s_8^2s_6s_5s_3fs_3, \\
r_3ft_0(r_6)^{-1} &= 1_H, \\
r_4f^2t_0(r_7)^{-1} &= 1_H, \\
r_{10}t_0(r_{10}s_6s_7s_4s_8s_4^{-1}k)^{-1} &= s_6s_7s_4^2ks_3^2f^2, \\
r_2fks_3t_0(r_2fs_3^{-1})^{-1} &= s_8^2s_6s_5s_8s_3s_5f^4, \\
r_3f^2t_0(r_5)^{-1} &= 1_H, \\
r_6t_0(r_6s_6s_7s_4^2s_3s_5fs_3)^{-1} &= s_8^2s_6s_7s_4^{-1}fs_4f^4, \\
r_7t_0(r_7s_8^2s_6s_7s_5^{-1}s_8s_3^2f^2k^3)^{-1} &= s_8^{-1}s_7s_4^{-1}s_5^{-1}s_3^{-1}s_4f^2k^3f, \\
r_{10}kt_0(r_4s_3^{-1}fs_3^{-1})^{-1} &= s_8^2s_7s_4s_9k^3s_3fks_3^{-1}, \\
r_{10}ft_0(r_{16})^{-1} &= 1_H, \\
r_{10}s_8^2s_6s_4s_9k^3ft_0(r_{13})^{-1} &= s_8s_4s_5ks_3fks_3^{-1}, \\
r_5t_0(r_5s_8^2s_5s_8s_3s_5fs_3^{-1})^{-1} &= s_8s_6s_4^{-1}s_8k^3s_3f^2k^3f, \\
r_6kt_0(r_3s_4s_5f)^{-1} &= s_8s_7s_4s_5s_3fkfs_3, \\
r_6ft_0(r_{17})^{-1} &= 1_H, \\
r_7kt_0(r_4s_6s_7s_5^{-1}s_8k^3f^2)^{-1} &= s_8^2s_5^{-1}k^3fs_4f^4, \\
r_7ft_0(r_{15})^{-1} &= 1_H,
\end{aligned}$$

$$\begin{aligned}
r_{10}f^2t_0(r_{18})^{-1} &= 1_H, \\
r_{16}t_0(r_{16}s_8^{-1}s_7s_4s_9s_5s_3fs_3)^{-1} &= s_7s_4^{-1}s_8s_3s_5fk s_3^{-1}, \\
r_{13}t_0(r_{13}s_8^{-1}s_5^{-1}s_8s_3s_5fk^3)^{-1} &= s_8s_9s_5s_3kf^4k^3, \\
r_5kt_0(r_3s_8s_6s_7s_4^{-1}s_3^{-1}s_4fs_3)^{-1} &= s_7s_5s_4^{-1}k, \\
r_5ft_0(r_{11})^{-1} &= 1_H, \\
r_6f^2t_0(r_{14})^{-1} &= 1_H, \\
r_{17}t_0(r_{17}s_4kfs_4f^4)^{-1} &= s_6s_5^{-1}s_3s_5fkfs_3, \\
r_4fk s_3t_0(r_4s_6s_7s_4^2fs_3^{-1})^{-1} &= s_4^2s_9s_8ks_3^{-1}f^2k^3f, \\
r_7s_9s_3^{-1}fs_3^{-1}t_0(r_{12})^{-1} &= s_8s_6s_4^{-1}s_5^{-1}s_3^{-1}s_4f^2k^3f, \\
r_7f^2t_0(r_{11}s_8^2s_6s_4s_8s_4^{-1}ks_3^{-1}fk s_3^{-1})^{-1} &= s_8^2ks_3f^2k^3f, \\
r_{15}t_0(r_{15}s_8^2s_7s_4^2s_3s_5fs_3)^{-1} &= s_7s_5s_9s_3fk s_3^{-1}, \\
r_{18}t_0(r_{18}s_8^{-1}s_6s_4^2s_3s_5fs_3)^{-1} &= s_8s_6s_7s_5s_8s_9s_3ks_3^{-1}f^2, \\
r_{16}kt_0(r_{10}s_8^{-1}s_6s_7s_9s_8fs_4)^{-1} &= s_7s_4^{-1}s_8s_3s_5fk s_3^{-1}, \\
r_{16}ft_0(r_{19})^{-1} &= 1_H, \\
r_6s_8s_6s_7s_4^2s_3^{-1}s_4fs_3t_0(r_9)^{-1} &= s_8^2s_4^{-1}k^3fs_4f^4, \\
r_{16}s_8^2s_6s_7s_5s_9k^2ft_0(r_{20})^{-1} &= s_8^2s_6s_7s_4s_9ks_3fs_3, \\
r_4s_8s_7s_4s_8s_4^{-1}s_3f^4kt_0(r_3s_8^2s_4s_5s_3^2s_4fs_3f)^{-1} &= s_8^2s_6s_7s_4s_5k, \\
r_{13}kt_0(r_{10}s_8^{-1}s_7s_4kfs_4)^{-1} &= s_6s_7s_5^{-1}s_8s_3s_5fkfs_3, \\
r_{13}ft_0(r_{18}s_5k^3fk^3s_3)^{-1} &= s_8^{-1}s_6s_5s_4^{-1}kfkfs_3, \\
r_5s_6s_4^{-1}s_5^{-1}k^2f^4t_0(r_6s_8^2s_7s_4s_5^{-1}s_3^2s_4fs_3f)^{-1} &= s_5s_9s_8s_3kfkfs_3, \\
r_3s_8s_4s_8s_4^{-1}k^3s_3f^4k^3t_0(r_4s_8^2s_7s_4s_5^{-1}s_3^2s_4fs_3f)^{-1} &= s_8^2s_5^2, \\
r_{11}t_0(r_{11}s_8^2s_7s_4kfs_4f^4)^{-1} &= s_5s_9, \\
r_{14}t_0(r_9s_3^{-1}s_4fs_3)^{-1} &= s_8s_6s_5^{-1}s_8s_3^2s_4f^4k^3, \\
r_{17}kt_0(r_6s_8s_6s_4s_8s_4^{-1}kf)^{-1} &= s_8^2s_6s_7s_4s_5s_9fs_4f^4, \\
r_{17}ft_0(r_{22})^{-1} &= 1_H, \\
r_7s_3f^2s_3t_0(r_7s_8^2s_6s_7s_5^2s_3ks_3^{-1}f^4)^{-1} &= s_8^2s_6s_9s_4s_5s_3s_5fkf^4, \\
r_{12}t_0(r_{12}s_8^2s_7s_9s_3s_5f^4)^{-1} &= s_8^2s_7s_4^2kf^2s_3, \\
r_{11}s_8^2s_6s_4s_8s_4^{-1}ks_3^{-1}fk s_3^{-1}t_0(r_{11}s_5s_8s_3ks_3^{-1})^{-1} &= s_8^{-1}s_7s_4^{-1}s_5^{-1}ks_3^{-1}, \\
r_{15}kt_0(r_7s_8^{-1}kf)^{-1} &= s_8^{-1}s_7s_5s_9s_8k^2, \\
r_{15}ft_0(r_{22}s_4^2ks_3^2fs_3)^{-1} &= s_8^{-1}s_6s_4^{-1}s_5^{-1}ks_3^2, \\
r_{16}s_3^{-1}s_4fs_3^{-1}t_0(r_{16}s_8^2s_7s_4^2s_3s_5fk^3)^{-1} &= s_8^2s_7s_4s_5^{-1}k^3f^2s_3, \\
r_{18}kt_0(r_{10}s_8^2s_6s_7s_4k^2f^2)^{-1} &= s_7s_5s_9s_3fk s_3^{-1}, \\
r_{18}ft_0(r_{22}s_8^{-1}s_4^{-1}f^4k^3)^{-1} &= s_8^{-1}s_6s_7s_5s_9s_4fs_3, \\
r_{16}kft_0(r_{17}s_8s_7s_5s_3fs_3f)^{-1} &= s_8s_6s_4s_9s_5s_3s_5fk^3f^4, \\
r_{16}f^2t_0(r_{19}s_8^{-1}s_6s_9ks_3)^{-1} &= s_8^{-1}s_7s_5^{-1}ks_3^2fk^3s_3, \\
r_{19}t_0(r_{20}s_6s_7s_5s_9s_3s_5f^4k)^{-1} &= s_7s_4^2s_9s_8fk^3s_3, \\
r_{13}s_8^2s_4s_5s_3kfs_3t_0(r_{16}s_6s_5s_8s_9s_3f^4)^{-1} &= s_6s_4s_8s_9s_3^{-1}f^2s_3, \\
r_9t_0(r_{14}s_8^{-1}s_6s_4^2s_3s_5fs_3)^{-1} &= s_7s_5s_9s_3^{-1}s_4f^2k^3f,
\end{aligned}$$

$$\begin{aligned}
r_{17}s_8^2s_7s_4s_8s_3kfs_3^{-1}t_0(r_{19}s_6s_5s_8s_9s_3f^4)^{-1} &= s_8s_4^2s_9s_3s_5fk^3f^4k, \\
r_{18}s_8^{-1}s_4s_5^{-1}kft_0(r_{21})^{-1} &= s_8^{-1}s_6s_9s_8s_4^{-1}s_3s_5fkfs_3^{-1}, \\
r_{20}t_0(r_{19}s_5^{-1}ks_3^{-1}fk^3)^{-1} &= s_7s_3^{-1}fk^3f^4k, \\
r_{18}s_5k^3fk^3s_3t_0(r_{16}s_8^2s_7s_4^2s_9k^3s_3fkf^4k)^{-1} &= s_8^2s_5s_8s_9ks_3fkfs_3, \\
r_{6}s_8^2s_7s_4s_5^{-1}s_3^2s_4fs_3ft_0(r_6s_7s_4^2ks_3f^4k)^{-1} &= s_6s_7s_4^2s_9s_8ks_3^{-1}f^2k^3f, \\
r_{17}s_8s_4^2s_9k^3fs_4t_0(r_{17}s_6s_5^2ks_3^2fs_3^{-1})^{-1} &= s_8s_6s_7s_4s_5^{-1}k^3s_3fkf^4, \\
r_{11}kt_0(r_5s_8^2s_6s_7s_5^2fk)^{-1} &= (s_4^{-1}s_3s_4)^2, \\
r_{11}ft_0(r_{15}s_7s_9s_8s_3s_5f^4k^3)^{-1} &= s_8^{-1}s_6s_4^2s_9s_3kfkfs_3^{-1}, \\
r_{14}kt_0(r_6s_8^{-1}s_6s_5s_9s_4s_3^{-1}s_4fs_3)^{-1} &= s_8^2s_6s_7s_4s_9k, \\
r_{14}ft_0(r_{20}s_8s_6s_7s_4s_9s_5s_3fk^3)^{-1} &= s_6s_9ks_3^2fkfs_3^{-1}, \\
r_9s_3^{-1}s_4fs_3t_0(r_6f^2)^{-1} &= s_8^2s_4s_5k^3s_3f^2s_3, \\
r_{17}f^2t_0(r_{22}s_8s_7s_4k^3s_3f^4k^3)^{-1} &= s_6s_5^{-1}s_8k^3s_3fkf^4k, \\
r_{22}t_0(r_{22}s_8s_4^2s_9k^2fk^3s_3)^{-1} &= s_8^{-1}s_6s_9s_5s_3s_5fk^3f^4, \\
r_{15}s_8^{-1}s_7s_4s_8fs_4t_0(r_{21}s_8^{-1}s_5s_8kfs_3^{-1})^{-1} &= s_8^{-1}s_7s_4s_8s_3^2f^4k^3f^4, \\
r_{16}s_8s_6s_7s_4^2s_3^{-1}s_4fs_3t_0(r_{22}s_8^2s_6s_7s_9s_4s_3fk^3s_3)^{-1} &= s_8^2s_7s_4^2s_9s_8k^2f^2k^3, \\
r_{12}kt_0(r_7s_8s_7s_5^2s_3^{-1}fs_3^{-1})^{-1} &= s_8s_6s_5s_8ks_3^{-1}f^2k^3f, \\
r_{12}ft_0(r_{22}s_8^{-1}s_6s_5^{-1}s_3^2f^4k^4)^{-1} &= s_8s_6s_4s_9k^3fs_3f, \\
r_{11}s_8s_4^2ks_3^{-1}fs_3t_0(r_7s_4f^2)^{-1} &= s_8^{-1}s_4ks_3^2fkfs_3^{-1}, \\
r_{11}s_8s_6s_4s_8s_3kfk^3s_3t_0(r_{20}s_8s_6s_7s_4s_9s_5ks_3f)^{-1} &= s_8s_6s_7s_4s_5s_3^2f^4, \\
r_{15}f^2t_0(r_{20}s_8s_6s_7s_4^2kfkf^4)^{-1} &= s_8s_7s_5s_9k^2fs_3, \\
r_{22}s_4^2ks_3^2fs_3t_0(r_{21}s_6s_7s_4s_8s_4^{-1}ks_3^{-1}f^2)^{-1} &= s_8s_6s_5s_4^{-1}ks_3^{-1}fs_4, \\
r_{12}s_8^{-1}s_6s_7s_5^2ks_3t_0(r_{17}s_8^2s_6s_5s_9k^3s_3fkfs_3^{-1})^{-1} &= s_6s_9s_4ks_3^{-1}f^2s_3, \\
r_{10}s_8s_4s_8s_4^{-1}k^3s_3f^4k^3t_0(r_{10}s_7s_4s_5^{-1}s_3f^4)^{-1} &= s_8s_5s_8ks_3^{-1}f^2k^3f, \\
r_{18}s_8^2s_6s_9s_3^{-1}fs_3^{-1}t_0(r_{18}s_4^{-1}s_3^{-1})^{-1} &= s_8^2s_5s_9s_3^2, \\
r_{18}s_8^{-1}s_6s_9s_3^2fkfs_3t_0(r_{22}s_8^{-1}s_5^{-1}s_8ks_3^2fkfs_3)^{-1} &= s_8s_6s_7s_4s_8s_9ks_3fs_3f, \\
r_{18}f^2t_0(r_{20}s_8^2s_4s_8s_3s_5fkfs_3)^{-1} &= s_8s_7s_5ks_3^2fkf^4k, \\
r_{22}s_8^{-1}s_4^{-1}f^4k^3t_0(r_{22}s_8^2s_6s_5ks_3^2fkf^4)^{-1} &= s_8^{-1}s_6s_7s_5s_4^{-1}s_3kfk^3s_3, \\
r_{17}s_8s_7s_5s_3fs_3ft_0(r_{16}s_8^2s_7s_4^{-1}s_5^{-1}kfk^3)^{-1} &= s_8^2s_7s_4^{-1}s_5^{-1}s_3fk^3f^4k, \\
r_{19}s_8^{-1}s_6s_9ks_3t_0(r_{22}s_8s_7s_5s_9s_8k^3s_3fkf)^{-1} &= s_6s_5^{-1}s_8s_3ks_3^{-1}f^2, \\
r_{19}kt_0(r_{16}s_8s_6s_7s_4s_8s_9f)^{-1} &= 1_H, \\
r_{20}s_6s_7s_5s_9s_3s_5f^4kt_0(r_{16}f)^{-1} &= s_8^2s_4s_8s_9k^3s_3f^4, \\
r_{16}s_6s_5s_8s_9s_3f^4t_0(r_{18}s_8^{-1}s_7s_9s_4k^2f^2s_3)^{-1} &= s_8s_5s_9s_8k^2, \\
r_9ft_0(r_{17}s_8^2s_6s_9s_8k^3s_3f^4k)^{-1} &= s_8^2s_6s_7s_5s_4^{-1}k^3fkf^4, \\
r_{17}s_8s_4^{-1}ks_3^2f^4t_0(r_{20}s_6s_9s_4k^3fs_3^{-1})^{-1} &= s_6s_9s_3^2fk^3f, \\
r_{19}s_6s_5s_8s_9s_3f^4t_0(r_{19}s_8^2s_7s_4^2s_9k^3s_3fkf^4k)^{-1} &= s_8^2s_6s_7s_4^{-1}s_8ks_3fkf^4, \\
r_{21}t_0(r_{21}s_8^2s_5s_9s_8s_3kfk)^{-1} &= s_6s_4s_8s_3ks_3^{-1}f^2k^3f, \\
r_{20}ft_0(r_{20}s_8^{-1}s_4s_8ks_3^{-1}fs_4)^{-1} &= s_4fk^3f^4, \\
r_{18}s_8^{-1}s_4^{-1}s_5^{-1}ks_3fk^3f^4t_0(r_{13}s_8^{-1}s_4^2s_9fs_3^{-1})^{-1} &= s_8s_6s_4s_5ks_3fkfs_3^{-1},
\end{aligned}$$



$$\begin{aligned}
r_{16}s_8^2s_7s_4^2s_9k^3s_3fkf^4kt_0(r_{13}f)^{-1} &= s_6s_4s_9s_3^{-1}, \\
r_{6}s_8s_7s_4s_5^{-1}fk s_3t_0(r_5s_8^2s_5^{-1}s_8k^3f^4)^{-1} &= s_8^2s_6s_7s_9s_8s_4^{-1}s_3^{-1}fkfs_3^{-1}, \\
r_{17}s_8s_4^2s_3^{-1}s_4fs_3t_0(r_{12}f)^{-1} &= s_8^{-1}s_5^2s_3^{-1}f, \\
r_{15}s_7s_9s_8s_3s_5f^4k^3t_0(r_{15}s_6s_7s_4^{-1}s_8ks_3f^4)^{-1} &= s_7s_4^2ks_3^2f^2, \\
r_9s_8^2s_6s_7k^3s_3fk^3s_3t_0(r_{18}s_8s_6s_7s_5s_8s_9fkf^4)^{-1} &= s_8^2s_7s_9s_5k^3s_3fk s_3^{-1}, \\
r_{14}s_6s_7s_9s_8s_3fs_3ft_0(r_{22}s_8^2s_7s_9s_3^{-1}f^4k^3)^{-1} &= s_8^{-1}s_6s_7s_4^{-1}s_5^{-1}ks_3^2fkfs_3, \\
r_{14}f^2t_0(r_{14}s_7s_9s_5s_3kfs_3)^{-1} &= s_8s_6s_5s_9s_4k^2fk^3f^4, \\
r_{20}s_8s_6s_7s_4s_9s_5s_3fk^3t_0(r_{20}s_8s_7s_4s_5^{-1}s_3^{-1}f)^{-1} &= s_6s_9s_4fk^3f^4, \\
r_{22}s_8s_7s_4k^3s_3f^4k^3t_0(r_{12}s_3f^4k^3f^4)^{-1} &= s_3^2k^3s_3f, \\
r_{22}kt_0(r_{17}s_6s_4s_5^{-1}k^2f)^{-1} &= s_8^2s_6s_7s_4s_9k, \\
r_{22}ft_0(r_{18}s_6s_7s_5s_3kfs_4)^{-1} &= s_8^{-1}s_4^2s_3ks_3^{-1}f^2k^3f, \\
r_{11}s_8^{-1}s_7s_5s_9s_8s_3fs_3^{-1}t_0(r_{14}s_9s_3kfs_3)^{-1} &= s_7s_4^{-1}s_5^{-1}s_3^{-1}fk s_3^{-1}, \\
r_{15}s_8s_4^2s_3^{-1}s_4fs_3t_0(r_{18}s_8^{-1}s_7s_4s_8s_4^{-1}ks_3^2)^{-1} &= s_8^{-1}s_6s_9s_4ks_3^2fkf, \\
r_{21}s_8^{-1}s_5s_8kfs_3^{-1}t_0(r_{22}s_8^{-1}s_7s_4^{-1}s_8s_3s_5fk s_3f^4)^{-1} &= s_8^2s_6s_7s_5ks_3^{-1}f^4k^3, \\
r_{18}s_6s_7s_4ks_3^{-1}fs_3t_0(r_{15}s_8^2s_7s_9s_4s_5k^3fk^3f^4)^{-1} &= s_8s_6s_7s_4^2s_9k^2fs_3^{-1}, \\
r_{22}s_8^2s_6s_7s_9s_4s_3fk^3s_3t_0(r_{19}s_7s_4s_8s_4^{-1}fs_3)^{-1} &= s_6s_5s_9s_4s_3ks_3^{-1}f^4k^3f^4, \\
r_{10}s_8s_7s_4s_8s_4^{-1}s_3f^4kt_0(r_7s_4^{-1}s_5^{-1}s_3^2s_4fs_3f)^{-1} &= s_8^{-1}s_6s_7s_4s_5k^3, \\
r_{22}s_8^{-1}s_6s_5^{-1}s_3^2f^4kf^4t_0(r_{17}s_8s_4^2s_3^{-1}s_4fs_3)^{-1} &= s_8s_6s_4^2s_3fk^3f^4k, \\
r_7s_8s_4s_8s_4^{-1}k^3s_3f^4k^3t_0(r_{10}s_8^2s_7s_4s_5^{-1}s_3^2s_4fs_3f)^{-1} &= s_8^2s_6, \\
r_{20}s_8s_6s_7s_4^2kfkf^4t_0(r_{18}s_8^{-1}s_6s_7s_5^{-1}s_8kf^2k^3)^{-1} &= s_8^{-1}s_6s_7s_4s_8s_9ks_3^{-1}f^4k, \\
r_{22}s_8s_6s_7s_5^{-1}ks_3^{-1}f^2k^3t_0(r_{15}s_8^{-1}s_4s_8s_4^{-1}kf)^{-1} &= s_7k^3f^2, \\
r_{21}s_6s_7s_4s_8s_4^{-1}ks_3^{-1}f^2t_0(r_{15}f)^{-1} &= s_8s_6s_7s_5s_8s_3^2s_4fs_3, \\
r_{18}s_8^{-1}s_5^{-1}s_8s_3^2f^4t_0(r_{18}s_8^{-1}s_7s_4s_5s_3^2f^4)^{-1} &= s_6s_4^2s_9s_8k^3fs_4f^4, \\
r_{18}s_8^2s_6s_7s_9s_5fkf^4kt_0(r_9s_8^2s_4s_8s_4^{-1}k^3s_3fs_3^{-1})^{-1} &= s_8s_6s_4s_3s_5fs_3, \\
r_{22}s_8^{-1}s_5^{-1}s_8ks_3^2fk s_3t_0(r_{22}s_8^{-1}s_7s_4s_5ks_3^2fs_3^{-1})^{-1} &= s_8s_4s_5ks_3^2fk, \\
r_{18}s_6s_7s_4s_8s_3s_5fs_3^{-1}t_0(r_{14}s_8^{-1}s_6s_4^2s_9ks_3f^4kf^4)^{-1} &= s_8s_4s_5^{-1}k, \\
r_{20}s_8^2s_4s_8s_3s_5fk s_3t_0(r_{15}s_6s_5^2s_3^2s_4)^{-1} &= s_8^{-1}s_6s_7s_4s_5s_9k^2fs_3f, \\
r_{17}s_7s_4s_3f^2s_3t_0(r_{22}s_8s_6s_4^{-1}s_8k^3s_3f^2)^{-1} &= s_8^2s_7s_9s_5f, \\
r_{19}s_7s_4^2s_9s_8s_3^{-1}t_0(r_{16}s_8^{-1}s_7s_5s_9s_4s_3^{-1}s_4fs_3)^{-1} &= s_8^2s_6s_5^2s_3kfk^3, \\
r_{22}s_8s_7s_5s_9s_8k^3s_3fkft_0(r_{16}f^2)^{-1} &= s_8^{-1}s_7s_4s_5k^2fk s_3^{-1}, \\
r_{19}kft_0(r_{17}s_8s_6s_4^2s_3kfs_3^{-1})^{-1} &= s_8s_4s_8s_9ks_3fk s_3, \\
r_{17}s_8^2s_7s_5^2fs_3^{-1}t_0(r_{14}s_8^2s_7s_4s_8s_3f^4k^3)^{-1} &= s_8^2s_6s_7s_4^2s_9s_8k^3fs_4f^4, \\
r_{17}s_8^2s_6s_9s_8k^3s_3f^4kt_0(r_{17}s_8s_6s_7s_4^2s_9s_3fk^3f^4)^{-1} &= s_5s_8kfs_4f^4, \\
r_{20}s_6s_9s_4k^3fs_3^{-1}t_0(r_{22}s_6s_7s_4s_9k^3s_3f^2)^{-1} &= s_8^{-1}s_6s_4^2s_9s_3ks_3^{-1}f^4k, \\
r_{19}s_6s_5s_8s_9s_3t_0(r_{19}s_6s_7s_5s_8s_3fk^3s_3)^{-1} &= s_8^{-1}s_4s_8s_4^{-1}s_3ks_3^{-1}f^4kf^4, \\
r_{22}s_8^2s_6s_7s_4s_9ks_3^{-1}fkfs_3t_0(r_{18}s_8s_6s_4s_8s_4^{-1}s_3kfs_4f^4)^{-1} &= s_8^{-1}s_6s_7s_4^{-1}s_8s_3fkf, \\
r_{18}s_8^2s_4s_3ks_3^{-1}f^4t_0(r_{18}s_7s_5^2s_3ks_3^{-1}f^4)^{-1} &= s_8^{-1}s_6s_7s_9s_5k^3s_3fkfs_3, \\
r_{21}kt_0(r_{18}s_8^{-1}kf)^{-1} &= s_8s_5s_3^2f^2k^3,
\end{aligned}$$

$$\begin{aligned}
r_{19}s_8s_7s_9s_8s_3s_5fk s_3t_0(r_{19}s_6s_7s_5s_8s_3)^{-1} &= s_8^2s_3^{-1}f^2k^3, \\
r_{20}kft_0(r_{14}s_8s_4^{-1}f)^{-1} &= s_8^2s_7s_9s_8k^3s_3f^4k^3f^4, \\
r_{20}fkt_0(r_{11}s_8^{-1}s_7s_5^2kfk s_3^{-1})^{-1} &= s_8s_6s_7s_9s_5s_3^2f^4k, \\
r_{20}f^2t_0(r_{21}s_8s_7s_4^2s_9s_8k^3f^2)^{-1} &= s_8^2s_6s_7s_4^{-1}s_5^{-1}s_3s_5f^2, \\
r_{19}s_8^{-1}s_9s_8s_4^{-1}k^3f^4t_0(r_8)^{-1} &= s_7s_4^2s_9s_8s_3^2fkf s_3^{-1}, \\
r_{19}s_8s_6s_7s_4s_9s_5k^3f^4t_0(r_{21}s_8^{-1}s_7s_4s_9k^3f^4)^{-1} &= s_7s_4^2s_9s_8fk^3f^4k, \\
r_{22}s_6s_5s_9s_8k^3f s_3t_0(r_{20}s_8^2s_6s_7s_4s_8s_4^{-1}kfk s_3)^{-1} &= s_8^{-1}s_6s_7s_4s_9k s_3^2fkf s_3, \\
r_{20}s_8^2s_6s_4^{-1}s_3^2s_4fkf^4k t_0(r_{22}s_8^2s_5s_4^{-1}kf)^{-1} &= s_8^2s_7s_9s_4s_5k s_3^2fkf^4k, \\
r_{14}s_7s_4k s_3^{-1}f s_3t_0(r_{11}s_8^2s_6s_5s_8fk^3f^4)^{-1} &= s_8^{-1}s_7s_4s_8s_9k^3s_3f s_3^{-1}, \\
r_{17}s_8^2s_7k^3s_3f^4t_0(r_9s_8s_6s_5s_9f)^{-1} &= s_6s_7s_4^{-1}fk^3f^4k, \\
r_{15}s_7s_9s_8s_3s_5f^4t_0(r_{11}s_8s_6s_4s_8s_4^{-1}kf)^{-1} &= s_8^2s_7s_9s_8fk s_3f^4, \\
r_{14}s_8^{-1}s_6s_7s_4s_8s_4^{-1}fkf^4k t_0(r_{18}s_6s_4s_9s_5s_3^{-1}f s_3f)^{-1} &= s_8^{-1}s_5^{-1}s_8k s_3^{-1}f^2k^3f, \\
r_{22}s_8^2s_7s_9s_3^{-1}f^4k^3t_0(r_{22}s_8^2s_7s_9s_4s_3^{-1}f^4)^{-1} &= s_8^2s_6s_7s_9s_8k^2f s_4f^4, \\
r_{20}s_6s_9s_8s_4^{-1}k^3fk^3s_3t_0(r_{17}s_3^2f^4k)^{-1} &= s_8^2s_7s_5s_4^{-1}s_3^2s_4fkf, \\
r_{22}s_8^2s_7s_4s_8fkf^4t_0(r_{21}s_8^2s_6s_7s_4s_9k^2f^4k)^{-1} &= s_8^2s_5s_8k^3s_3f s_4f^4, \\
r_{21}s_5^{-1}s_8k s_3^{-1}f^2s_3t_0(r_{19}s_8^{-1}s_6s_4s_8k s_3^{-1}fk s_3)^{-1} &= s_8s_6s_4s_8s_9s_3k s_3^{-1}f s_3, \\
r_{17}s_8^2s_6s_7s_4^{-1}s_5^{-1}s_3^2s_4f s_3f t_0(r_{17}s_8^{-1}s_6s_7s_5^{-1}s_8s_3f^4k)^{-1} &= s_8^2s_6s_5s_8s_3kf^2k^3f, \\
r_{19}s_8s_7s_4s_5^{-1}k s_3^{-1}t_0(r_{21}s_8s_5s_8s_3s_5f s_3^{-1})^{-1} &= s_8^{-1}s_7s_4^2k^3s_3f, \\
r_{11}s_5^{-1}s_8k^3fk^3s_3t_0(r_{11}s_5s_4^{-1}s_3s_5f^4k^3)^{-1} &= s_8^2s_6s_7s_5s_8s_9k^3s_3fkf s_3^{-1}, \\
r_{22}s_8s_6s_7s_4s_8s_9s_3^2s_4f s_3^{-1}t_0(r_{14}s_8^{-1}s_7s_5^2f^4k^3)^{-1} &= s_8^2s_6s_7s_5^{-1}s_8s_3f s_3f, \\
r_{22}s_8^2s_7s_4k s_3^{-1}fkf t_0(r_{20}s_8^2s_5s_3^2)^{-1} &= s_7s_9s_5s_3kf s_3^{-1}, \\
r_{14}s_8^2s_7s_4s_8s_3f^4k^3t_0(r_{17}s_8s_7s_4s_8s_4^{-1}fk s_3)^{-1} &= s_8^2s_7s_5s_8s_9k s_3fkf s_3, \\
r_{22}s_7s_9s_4kf s_3t_0(r_{17}s_7s_9s_4k s_3f s_3^{-1})^{-1} &= s_6s_7s_9s_4k^2f^4k^3, \\
r_{21}s_8^2s_5s_3^2fk s_3^{-1}t_0(r_{21}s_8s_6k^3s_3f^2)^{-1} &= s_7s_4^2s_9fk^3f^4k, \\
r_{19}s_8^2s_6s_4^{-1}s_3f^2s_3t_0(r_{21}s_6s_7s_4s_5s_3^2s_4f^4k^3)^{-1} &= s_4s_5s_9s_3kf k f s_3^{-1}, \\
r_{21}s_6s_4s_9k^3f t_0(r_{22}s_8s_6s_7s_5^{-1}k s_3^{-1}fkf)^{-1} &= s_8^2s_6s_7s_5^2s_3^{-1}s_4fk^3f, \\
r_{21}s_8s_6s_7s_4^{-1}s_3fk^3t_0(r_{20}s_8^2s_3^{-1}fk s_3^{-1})^{-1} &= s_6s_7s_4s_8s_3kf k^3f^4, \\
r_{21}s_8s_7s_5s_9s_8k^3s_3f^2t_0(r_{21}s_8s_6s_5s_9s_8k^3s_3f^2)^{-1} &= s_8^2s_4s_8s_9s_3k s_3^{-1}f s_3, \\
r_8t_0(r_{21}s_8^{-1}s_6s_5s_8kf^4)^{-1} &= s_6s_5^2s_3^{-1}s_4f^4kf^4, \\
r_{21}s_8s_6s_7s_5s_8s_9k^3f^4k t_0(r_8s_8s_7s_5fk^3f^4)^{-1} &= s_8s_6s_4^{-1}s_5^{-1}s_3^2s_4f^4, \\
r_{21}s_8s_5s_8s_3s_5f s_3^{-1}t_0(r_{19}s_8^2s_6s_7s_5s_8s_9s_3s_5f s_3^{-1})^{-1} &= s_8^{-1}s_9s_4s_5s_3f s_3f, \\
r_{21}s_8^2s_4s_3fk s_3t_0(r_{19}s_8s_6s_7s_4^2s_9s_3)^{-1} &= s_8^{-1}s_7s_4s_9s_5s_3fk, \\
r_8k t_0(r_{19}s_8^2s_7s_5^2s_3kf^2s_3)^{-1} &= s_7s_9s_5s_3^{-1}s_4fkf.
\end{aligned}$$

## Anhang C

# Eine konkrete Charaktertafel der Rudvalis-Gruppe

Für  $n \in \mathbb{N}$  bezeichne  $\zeta_n$  die primitive  $n$ -te Einheitswurzel  $\exp(\frac{2\pi i}{n})$  im Körper der komplexen Zahlen. Die auf Seite 102 abgedruckte konkrete Charaktertafel der Gruppe  $G \leq S_{593775}$  aus Satz 5.5.2 verwendet folgende Abkürzungen zur Darstellung irrationaler Werte:

$$\mathbf{A} := -\zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 - \zeta_7^6$$

$$\mathbf{B} := \zeta_7 - \zeta_7^2 + \zeta_7^3 + \zeta_7^4 - \zeta_7^5 + \zeta_7^6$$

$$\mathbf{C} := \zeta_7 + \zeta_7^2 - \zeta_7^3 - \zeta_7^4 + \zeta_7^5 + \zeta_7^6$$

$$\begin{aligned} \mathbf{D} &:= -2\zeta_4 \\ &= -2i \end{aligned}$$

$$\begin{aligned} \mathbf{E} &:= -\zeta_5 + \zeta_5^2 + \zeta_5^3 - \zeta_5^4 \\ &= -\sqrt{5} \end{aligned}$$

$$\begin{aligned} \mathbf{F} &:= -\zeta_{24} + \zeta_{24}^{11} + \zeta_{24}^{17} - \zeta_{24}^{19} \\ &= -\sqrt{6} \end{aligned}$$

$$\mathbf{G} := -\zeta_{13} - \zeta_{13}^2 - \zeta_{13}^3 + \zeta_{13}^4 - \zeta_{13}^5 + \zeta_{13}^6 + \zeta_{13}^7 - \zeta_{13}^8 + \zeta_{13}^9 - \zeta_{13}^{10} - \zeta_{13}^{11} - \zeta_{13}^{12}$$

$$\mathbf{H} := -\zeta_{13} + \zeta_{13}^2 + \zeta_{13}^3 - \zeta_{13}^4 - \zeta_{13}^5 - \zeta_{13}^6 - \zeta_{13}^7 - \zeta_{13}^8 - \zeta_{13}^9 + \zeta_{13}^{10} + \zeta_{13}^{11} - \zeta_{13}^{12}$$

$$\mathbf{I} := \zeta_{13} - \zeta_{13}^2 - \zeta_{13}^3 - \zeta_{13}^4 + \zeta_{13}^5 - \zeta_{13}^6 - \zeta_{13}^7 + \zeta_{13}^8 - \zeta_{13}^9 - \zeta_{13}^{10} - \zeta_{13}^{11} + \zeta_{13}^{12}$$

$$\begin{aligned} \mathbf{J} &:= -\zeta_{29} - \zeta_{29}^4 - \zeta_{29}^5 - \zeta_{29}^6 - \zeta_{29}^7 - \zeta_{29}^9 - \zeta_{29}^{13} - \zeta_{29}^{16} - \zeta_{29}^{20} - \zeta_{29}^{22} - \zeta_{29}^{23} - \zeta_{29}^{24} - \zeta_{29}^{25} - \zeta_{29}^{28} \\ &= \frac{1}{2} (1 - \sqrt{29}) \end{aligned}$$

Ferner symbolisiert  $*$  den nicht-trivialen  $\mathbb{Q}$ -Automorphismus der Körpererweiterung  $\mathbb{Q}(\sqrt{29})$ .

[illegible]

# Literaturverzeichnis

- [1] ASSA, S. B.:  
*A Characterization of  ${}^2F_4(2)'$  and the Rudvalis Group*,  
Journal of Algebra **41** (1976), 473–495.
- [2] BOSMA, W., CANNON, J.:  
*The MAGMA Handbook (Release V2.7)*.  
<http://www.maths.usyd.edu.au:8000/u/magma>, Sydney, 2000.
- [3] BRAUER, R., FOWLER, K. A.:  
*On Groups of Even Order*,  
Annals of Mathematics **62(3)** (1955), 565–583.
- [4] BUTLER, G.:  
*Computing in Permutation and Matrix Groups II: Backtrack Algorithm*,  
Mathematics of Computation **39** (1982), 671–680.
- [5] BUTLER, G.:  
*Fundamental Algorithms for Permutation Groups*.  
Lecture Notes in Computer Science **559**, Springer-Verlag Heidelberg, 1991.
- [6] CANNON, J. J., HAVAS, G.:  
*Algorithms for Groups*,  
The Australian Computer Journal **24(2)** (1992), 51–60.
- [7] CONWAY, J. H., WALES, D. B.:  
*Construction of the Rudvalis Group of Order 145,926,144,000*,  
Journal of Algebra **27** (1973), 538–548.
- [8] CONWAY, J. H., CURTIS, R. T., NORTON, S. P., PARKER, R. A., WILSON, R. A.:  
*Atlas of Finite Simple Groups*.  
Clarendon Press Oxford, 1985.
- [9] COOPERMAN, G., FINKELSTEIN, L., TSELMAN, M., YORK, B.:  
*Constructing Permutation Representations for Large Matrix Groups*,  
Journal of Symbolic Computation **24** (1997), 471–488.
- [10] COOPERMAN, G., LEMPKEN, W., MICHLER, G. O., WELLER, M.:  
*A New Existence Proof of Janko's Simple Group  $J_4$* ,  
Progress in Mathematics **173** (1999), 161–175.

- [11] CURTIS, C. W., REINER, I.:  
*Representation Theory of Finite Groups and Associative Algebras.*  
Wiley (Interscience) NewYork, 1962.
- [12] DIXON, J. D.:  
*High Speed Computation of Group Characters,*  
Numerische Mathematik **10** (1967), 446–450.
- [13] GAP GROUP, THE:  
*GAP – Groups, Algorithms, and Programming (Version 4.2).*  
<http://www-gap.dcs.st-and.ac.uk/~gap>, Aachen, St Andrews, 2000.
- [14] GOLLAN, H. W., OSTERMANN, T. W.:  
*Operation of Class Sums on Permutation Modules,*  
Journal of Symbolic Computation **9** (1990), 39–47.
- [15] GOLLAN, H. W.:  
*A Contribution to the Revision Project of the Sporadic Groups: Lyons' simple group  $L_y$ ,*  
Vorlesungen aus dem Fachbereich Mathematik der Universität GH Essen **26** (1998).
- [16] HIGMAN, D. G.:  
*Intersection Matrices for Finite Permutation Groups,*  
Journal of Algebra **6** (1967), 22–42.
- [17] HUPPERT, B.:  
*Endliche Gruppen I.*  
Springer-Verlag Berlin Heidelberg, 1983.
- [18] ISAACS, I. M.:  
*Character Theory of Finite Groups.*  
Dover Publications New York, korrigierte Neuauflage 1994.
- [19] JANKO, Z.:  
*A New Finite Simple Group with Abelian Sylow 2-subgroups and its characterization,*  
Journal of Algebra **3** (1966), 147–186.
- [20] JANKO, Z.:  
*Some New Simple Groups of Finite Order, I,*  
Symposia Mathematica **1** (1968), 25–64.
- [21] JANKO, Z.:  
*A New Finite Simple Group of Order 86,775,571,046,077,562,880 which Possesses  $M_{24}$  and the Full Covering Group of  $M_{22}$  as Subgroups,*  
Journal of Algebra **42** (1976), 564–596.
- [22] KRATZER, M., MICHLER, G. O.:  
*A Natural Existence Proof for Janko's Sporadic Group  $J_1$ ,*  
RIMS Kokyuroku **1149** (2000), 39–52, Chiba University, Kyoto.
- [23] KRATZER, M.:  
*Uniform and Natural Existence Proofs for Janko's Sporadic Groups  $J_2$  and  $J_3$ ,*  
Archiv der Mathematik, zum Druck angenommen.

- [24] KURZWEIL, H., STELLMACHER, B.:  
*Theorie der endlichen Gruppen.*  
Springer-Verlag Berlin Heidelberg New York, 1998.
- [25] LEMPKEN, W.:  
*On Local and Maximal Subgroups of Janko's Simple Group  $J_4$ ,*  
Memorie di Matematica **107** (1989), 47–103.
- [26] LEMPKEN, W.:  
*More on the Simple Groups Related to  $M_{24}$ ,*  
in Vorbereitung.
- [27] LEMPKEN, W.:  
*Constructing 3ON by means of Involution Centralizers,*  
in Vorbereitung.
- [28] LENSTRA, A. K., LENSTRA, H. W., LOVÁSZ, L.:  
*Factoring Polynomials with Rational Coefficients,*  
Mathematische Annalen **261** (1982), 515–534.
- [29] LEON, J. S.:  
*Permutation Group Algorithms Based on Partitions, I: Theory and Algorithms,*  
Journal of Symbolic Computation **12** (1991), 533–583.
- [30] MICHLER, G. O.:  
*On the Construction of the Finite Simple Groups with a Given Centralizer of a 2-central Involution,*  
Journal of Algebra **234** (2000), 668–693.
- [31] MICHLER, G. O., WAKI, K., WELLER, M.:  
*Natural Existence Proof for Lyons' Simple Group,*  
IEM-Preprint No. **7** (2001), Universität GH Essen, Essen.
- [32] MICHLER, G. O., WELLER, M.:  
*A New Computer Construction of the Irreducible 112-dimensional 2-modular Representation of Janko's Group  $J_4$ ,*  
Communications in Algebra **29(4)** (2001), 1773–1806.
- [33] MICHLER, G. O., WELLER, M.:  
*The Character Values of the Irreducible Constituents of a Transitive Permutation Representation,*  
IEM-Preprint No. **14** (2000), Universität GH Essen, Essen.
- [34] PARKER, R. A.:  
*The Computer Calculation of Modular Characters: The Meat-Axe,*  
in *Computational Group Theory*  
(Herausgeber: ATKINSON, M. D.).  
Academic Press London, 1984, 267–274.
- [35] PARROT, D.:  
*A Characterization of the Rudvalis Simple Group,*  
Proceedings of the London Mathematical Society **32(3)** (1976), 25–51.

- [36] PLESKEN, W.:  
*Additively Indecomposable Integral Quadratic Forms*,  
Journal of Number Theory **47** (1994), 273–283.
- [37] RUDVALIS, A.:  
*A New Simple Group of Order  $2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$* ,  
Notices of the American Mathematical Society **20** (1973), A-95.
- [38] SCHNEIDER, G. J. A.:  
*Dixon's Character Table Algorithm Revisited*,  
Journal of Symbolic Computation **9** (1990), 601–606.
- [39] SCHÖNERT, M. et al.:  
*GAP – Groups, Algorithms, and Programming (Version 3.4.4)*.  
Lehrstuhl D für Mathematik, RWTH Aachen, Aachen, 5. Auflage 1995.
- [40] SIMS, C. C.:  
*Determining the Conjugacy Classes of a Permutation Group*,  
in *Proceedings of the Symposium on Applied Mathematics*  
(Herausgeber: BIRKHOFF, G., HALL, M., JR.).  
American Mathematical Society Providence, Rhode Island, 1971, 191–195.
- [41] SIMS, C. C.:  
*Computation with Permutation Groups*,  
in *Proceedings of the Second Symposium on Symbolic and Algebraic Manipulation*  
(Herausgeber: PETRICK, S. R.).  
Association of Computing Machinery New York, 1971, 23–28.
- [42] SULEIMAN, I. A. I., WALSH, P. G., WILSON, R. A.:  
*Conjugacy Classes in Sporadic Simple Groups*,  
Communications in Algebra **28(7)** (2000), 3209–3222.
- [43] THOMPSON, J. G.:  
*Finite-dimensional Representations of Free Products with an Amalgamated Subgroup*,  
Journal of Algebra **69** (1981), 146–149.
- [44] WELLER, M.:  
*Construction of Large Permutation Representations for Matrix Groups II*,  
Applicable Algebra in Engineering, Communications & Computing **11** (2001), 463–488.